L1 - Logique CUPGE

Jan-Georg Smaus

Université de Toulouse/IRIT

Année 2022/2023

Ce Cours

Ce cours a été donné par Olivier Gasquet avant 2014.
Depuis 2014/2015, Jan-Georg Smaus est le responsable de ce cours.
Entre 2017/2018 et 2020/2021 il a été accompagné par Ralph Matthes.
Le cours ressemble à Structures Discrètes 1 et la partie “Logique” de Structures Discrètes 2 données en Licence Informatique.
Olivier Gasquet, Ralph Matthes, Jean-Baptiste Raclet, Jan-Georg Smaus et Martin Strecker ont contribué aux transparents.

Organisation

Page moodle
https://moodle.univ-tlse3.fr/course/view.php?id=7986
Modalités de Contrôle
Il y aura trois contrôle écrits sur table :

- 16 février 18h, 16 mars 15h45, 23 mars 18h00
- durée 1 heure
- Note finale :

$$0.3 \cdot \max(CC1, CC3) + 0.3 \cdot \max(CC2, CC3) + 0.4 \cdot CC3$$

Plan

Problématique

Logique : du grecque logos (mot, énoncé, propos)

Histoire :

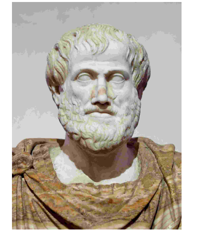
- Premiers développements au 4ème siècle av. J.-C.
- Scolastique médiévale : discipline essentielle (trivium : grammaire, rhétorique, logique)
- Refonte à la fin du 19ème siècle
- Crise au début du 20ème siècle

Objectifs de cette section :

- Connaître le développement historique de la discipline
- Apprécier ses limitations



Histoire de la logique : Aristote



Aristote (-384 .. -322)

- Disciple de Platon
- Précepteur d'Alexandre le Grand
- Contributions essentielles aux sciences naturelles, l'éthique, la logique
- "Le Philosophe" par excellence de la philosophie médiévale

Histoire de la logique : Aristote

Le syllogisme d'Aristote (1)

Instance :

- Prémisse majeure :
  Tous les hommes sont mortels
- Prémisse mineure :
  Tous les Grecs sont des hommes
- Conclusion :
  Tous les Grecs sont mortels

En général :

- Tous les B sont des C
- Tous les A sont des B
- Tous les A sont des C

Histoire de la logique : Aristote

Les syllogismes d'Aristote (2)

Observation essentielle :

- On peut reconnaître un argument valide par sa forme
- ...sans regarder la signification des mots
- ...énoncés de la forme : quantificateur (tous, aucun, certains,...)+sujet+verbe d'état+attribut du sujet

En terminologie moderne :

- On peut raisonner de manière syntaxique
- ...sans connaissance de la sémantique
- ...sur des propositions analysées simples



Histoire de la logique : Aristote

Les syllogismes d'Aristote (3)

Structure générale : deux prémisses, une conclusion

Quatre formes d'énoncé :

- Tout A est B (donc : $A \subseteq B$)
- Aucun A n'est B (donc : $A \cap B = \{\}$)
- Quelque A est B (donc : $A \cap B \neq \{\}$)
- Quelque A n'est pas B (donc : $A \not\subseteq B$)

Question

Lesquels des syllogismes suivants sont valides ?

- P_1 : Tout B est C
- P_2 : Quelque A est B
- C : Quelque A est C

- P_1 : Quelque B est C
- P_2 : Quelque A est B
- C : Quelque A est C

Les licornes ne peuvent pas voler, or je ne peux pas voler, donc je suis une licorne !

29 JANVIER

Logique et Intélligence

Il y a sans doute un rapport entre logique et intélligence, mais pour qu'une personne “joue le jeu” de la logique, ou bien de l'intélligence, elle a besoin d'une culture/éducation minimale, qui correspond à peu près à l'école élémentaire.

Logique et Intélligence

Il y a sans doute un rapport entre logique et intélligence, mais pour qu'une personne "joue le jeu" de la logique, ou bien de l'intélligence, elle a besoin d'une culture/éducation minimale, qui correspond à peu près à l'école élémentaire.

Question

"Tous les hommes sont mortels. Socrate est un homme. Que sait-on donc de Socrate ?"

Logique et Intélligence

Il y a sans doute un rapport entre logique et intélligence, mais pour qu'une personne “joue le jeu” de la logique, ou bien de l'intélligence, elle a besoin d'une culture/éducation minimale, qui correspond à peu près à l'école élémentaire.

Question

“Tous les hommes sont mortels. Socrate est un homme. Que sait-on donc de Socrate ?”
Une personne qui n'a jamais vu l'école élémentaire, que va-t-elle répondre typiquement à une telle question ?



Histoire de la logique : stoïciens et mégariques

La logique mégaro-stoïcienne date du 4ème siècle av. J.-C. et nous lui devons :

- Les connecteurs : disjonction, conjonction, négation, implication
- Les indémontrables :
  - Si A alors B. Or A. Donc B. (Modus Ponens)
  - Si A alors B. Or non B. Donc non A. (Modus Tollens)
  - A ou B. Or non A. Donc B. (avec “ou” inclusif)
  - A et B. Donc A.

Histoire de la logique : stoïciens et mégariques

- Si j'ai de la fièvre alors je suis malade. Or j'ai de la fièvre. Donc je suis malade.
- S'il pleut alors le sol est mouillé. Or le sol n'est pas mouillé. Donc il ne pleut pas.
- Tu as l'as de pique ou l'as de carreau. Or tu n'as pas l'as de carreau. Donc tu as l'as de pique.

NB : "Si ...alors ..." ne marque pas nécessairement une relation de cause à effet mais une simple simultanéité.
La fièvre ne cause pas la maladie (c'est même l'inverse), mais il n'y a pas de fièvre sans maladie alors qu'on peut être malade sans fièvre.
La fièvre est une condition suffisante pour la maladie.

Histoire de la logique : stoïciens et mégariques

Question

Quels raisonnements sont corrects ?

- Je prends l'avion si j'ai un bon tarif. Or je ne prends pas l'avion. Donc je n'ai pas eu un bon tarif.
- Je prends l'avion seulement si j'ai un bon tarif. Or je ne prends pas l'avion. Donc je n'ai pas eu un bon tarif.
- Je prends l'avion si et seulement si j'ai un bon tarif. Or je ne prends pas l'avion. Donc je n'ai pas eu un bon tarif.



Histoire de la logique : stoïciens et mégariques

Question

Quels raisonnements sont corrects ?

- Je prends l'avion si j'ai un bon tarif. Or je ne prends pas l'avion. Donc je n'ai pas eu un bon tarif.
- Je prends l'avion seulement si j'ai un bon tarif. Or je ne prends pas l'avion. Donc je n'ai pas eu un bon tarif.
- Je prends l'avion si et seulement si j'ai un bon tarif. Or je ne prends pas l'avion. Donc je n'ai pas eu un bon tarif.

Dans le premier raisonnement, un bon tarif est une condition suffisante pour prendre l'avion.
Dans le deuxième raisonnement, un bon tarif est une condition nécessaire pour prendre l'avion.
Le troisième est la combinaison des deux précédents.

Histoire de la logique : Leibniz

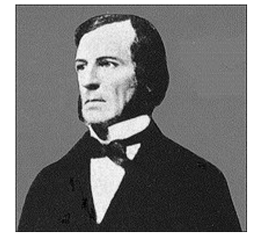


Leibniz (1646 - 1716)

- Codage binaire des nombres
- Construction de l'un des premiers calculateurs (mécanique, décimal)
- Développement du calcul infinitésimal (en concurrence avec Newton)
- Ars combinatoria : l'art de dériver des vérités de manière calculatoire, basé sur
  - une characteristica universalis, un langage mathématique non-ambigu
  - un calculus ratiocinator, un calcul / une machine manipulant la characteristica



Histoire de la logique : Boole

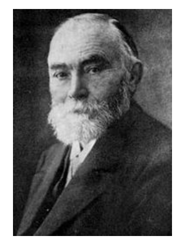


Boole (1815 - 1864)

Livre : An Investigation of the Laws of Thought

- Traitement algébrique de la logique propositionnelle
- Procédure de décision pour la logique propositionnelle

Histoire de la logique : Frege

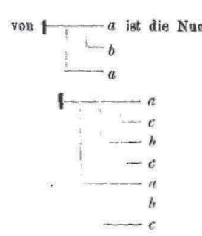


Frege (1848 - 1925)

- Fondateur de la logique "moderne" :
  - les connecteurs "essentiels" de la logique des propositions : $\longrightarrow$ et $\neg$
  - les quantificateurs de la logique des prédicats
  - un calcul formel

Histoire de la logique : Frege

"Begriffsschrift" de Frege (1879)



Les jugements

$\vdash a \longrightarrow b \longrightarrow a$

et

$\vdash (c \longrightarrow b \longrightarrow a) \longrightarrow ((c \longrightarrow b) \longrightarrow (c \longrightarrow a))$

- Distinction entre
  - formule : représente une proposition (qui peut être vraie ou fausse)
  - jugement : formule dont on constate la vérité (dans un calcul donné)
- Notation deux-dimensionnelle qui a laissé des traces :
  - négation ($\neg$)
  - jugement ($\vdash$)

Histoire de la logique : Russell



Russell (1872 - 1970)

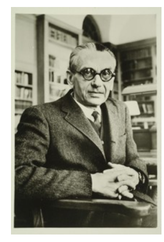
- Livre : Principia Mathematica (1910 - 1913, avec A. N. Whitehead)
  But : formalisation des mathématiques à partir de quelques notions élémentaires
- Découverte d'un paradoxe (1903) dans la théorie des ensembles de Cantor $\rightsquigarrow$ crise des fondements de la mathématique :
  Consistance des axiomes ?

Question

Le barbier se rase-t-il ou non ?



Histoire de la logique : Gödel



Gödel (1906 - 1978)

Le cataclysme : "Sur des propositions indécidables de Principia Mathematica" (1931)

- Toute théorie mathématique "suffisamment expressive" est
  - incomplète : il existe des énoncés vrais non-démontrables
  - ou contradictoire
- Surtout, elle ne permet pas de démontrer sa propre cohérence
- $\rightsquigarrow$ échec du programme rationaliste dans la tradition Leibniz - Hilbert

Histoire de la logique - Résumé

Quelques repères dans un paysage vaste :

- Syllogisme d'Aristote : Possibilité de raisonner en s'appuyant sur la syntaxe, sans connaissance de la sémantique
- Leibniz : Raisonnement exécutable par une machine (calcul)
- Forme moderne de la logique (Boole, Frege)
- Le programme rationaliste mis à mal : Russell, Gödel

Conclusion : La logique

- a des limites
- ne fournit pas de certitude absolue
- mais est pourtant utile . . .

Pour plus d'information sur le développement de la logique au tournant du 20ème siècle : Jean Van Heijenoort : From Frege to Gödel



Exercices (Syllogismes 1)

Question

Lesquels de ces syllogismes sont valides ?

- Aucun chat n'est humain. Aucun humain n'est bleu. Donc aucun chat n'est bleu.
- Les pies ont des plumes. Or les chats n'ont pas de plumes. Donc les chats ne sont pas des pies.
- Aucun chat n'est humain. Aucun non-humain n'a d'humour. Donc aucun chat n'a d'humour.
- Tout diptère est ailé. Or certains insectes ne sont pas ailés. Donc certains insectes ne sont pas diptères.

Résolvez-les par raisonnement ensembliste éventuellement graphique.
Diagrammes de Venn :

- jusqu'à 3 ensembles, au-delà c'est difficile
- existence (non vacuité) signalée par une croix

Exercices (Mégariques 1)

Question

Lesquels de ces raisonnements sont valides ?

- S'il y a du verglas, la route est glissante.
  Si la route est glissante, les camions ne roulent pas.
  Or les camions roulent.
  Donc il n'y a pas de verglas.
- Quand il ne pleut pas, le sol est sec.
  Quand il n'y a pas d'humidité dans l'air, il ne pleut pas.
  Or l'air est humide.
  Donc le sol n'est pas sec.

Exercices (Mégariques 2)

Pour adhérer à un club, tout candidat doit remplir les conditions 1 à 8 :

1. s'il joue de la cornemuse et s'il ne porte pas un kilt alors il n'est pas écossais
2. il joue au rugby ou il porte un kilt
3. s'il joue de la cornemuse et s'il ne joue pas au rugby alors il n'est pas écossais
4. il est écossais ou il joue de la cornemuse
5. s'il est écossais et s'il porte un kilt alors il joue de la cornemuse
6. s'il n'est pas écossais alors il ne joue pas de la cornemuse
7. s'il est écossais et s'il joue au rugby alors il joue de la cornemuse
8. s'il joue au rugby et s'il porte un kilt alors il ne joue pas de la cornemuse

Qui ne peut espérer adhérer à ce club ?

NB (Proverbe anglais) : "Un gentleman est un homme qui sait jouer de la cornemuse, mais qui n'en joue pas".

Plan

Applications de la logique

La logique a d’importantes applications en informatique :

- Intélligence artificielle
- Sûreté de fonctionnement : aérospatiale, production industrielle ...
- Sécurité : bourse, cryptomonnaie ...

Objectifs de cette section :

- Comprendre le rôle de la logique dans l’informatique
- Gagner une intuition des méthodes mises en œuvre

Application : Intélligence artificielle (1)

But :

- Comprendre mieux le fonctionnement de l'intelligence humaine
- Découvrir les facettes d'un comportement rationnel

Applications :

- Simuler le comportement humain :
  comportement grégaire en économie (rationalité $\pm$ réduite)
- Guider l'action humaine :
  aide au diagnostic (médical, informatique,...)
- Imiter le comportement humain :
  robotique, jeux classiques, jeux vidéos (personnages virtuels)

Application : Intélligence artificielle (1)

But :

- Comprendre mieux le fonctionnement de l'intelligence humaine
- Découvrir les facettes d'un comportement rationnel

Applications :

- Simuler le comportement humain :
  comportement grégaire en économie (rationalité $\pm$ réduite)
- Guider l'action humaine :
  aide au diagnostic (médical, informatique,...)
- Imiter le comportement humain :
  robotique, jeux classiques, jeux vidéos (personnages virtuels)

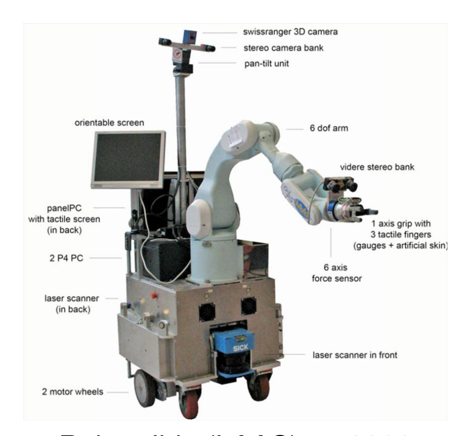
Programme ANITI à Toulouse (y compris l'UPS), un d'une poignée massivement soutenue par l'État en ce moment dans le cadre d'une grande initiative pour l'IA.



Application : Intélligence artificielle (2)

Robotique :

- Contrôle des actions :
  Comment déplacer un livre d'une chaise sur une table ?
- Contrôle des mouvements :
  Comment se déplacer d'une salle à une autre ?
- Interaction homme-machine :
  Comment interpréter une commande en langage naturel ?



Robot Jido (LAAS) en 2008

Application : Sûreté de fonctionnement (1)

But : S'assurer du bon fonctionnement du matériel et logiciel de systèmes critiques :

- Transport (avions, trains)
- Nucléaire
- Systèmes médicaux

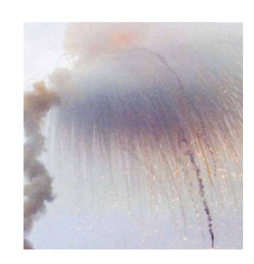
Contexte :

- Systèmes embarqués de plus en plus sophistiqués
- Exemple : Système fly by wire de l'A330



à lire : Wired: History's worst software bugs

Application : Sûreté de fonctionnement (2)



Explosion de la fusée Ariane 5 (juin 1996) :

- 40 sec. après son lancement
- À bord : 4 satellites de recherche
- Dispersion de 745 tonnes de débris, y compris substances toxiques
- Coût des dégats : 290 millions d'Euros

Contexte :

- Premier lancement de la fusée
- Lors du développement : Réutilisation de logiciel de l'Ariane 4 (autres caractéristiques de vol, accéleration moins forte)
- Cause : dépassement arithmétique

Application : Sûreté de fonctionnement (3)

- Exemple du domaine médical : Therac-25 (entre 1985 et 1987)
  - Lors d'une radiothérapie, 6 personnes reçoivent une surdose massive (facteur 100)
  - Conséquence : 3 décès
  - Causes : Multiples, surtout :
    problème de synchronisation de deux tâches
- Mai 2007, à Toulouse :
  - 145 personnes irradiés au CHU de Rangueil
    "c'est encore une fois une déficience de l'informatique qui serait en cause [...] L'étalonnage était mal fait [...]"
  - lire l'article dans le Parisien



Application : Robots dans l'Industrie

Les carrosseries des voitures sont assemblées par des robots ces jours-là.
Un robot pourrait facilement tuer un humain travaillant sur le même site.
Vérification pertinente.

Application : Sécurité

Problème :

- Des virus et vers informatiques infectent des systèmes connectés par Internet
- Exemple : Ver “Slammer” (janvier 2003)
  - infecte 75.000 machines en 30 min
  - entre autres : blocage du système de surveillance de la centrale nucléaire Davis-Besse (Ohio) pendant 5h

Causes de la vulnérabilité :

- Langages de programmation de bas niveau (assembleur, C)
- Incompréhension du fonctionnement des protocoles de communication
- Cryptage insuffisant

à lire : Wired: Slammer



Application : La Bourse

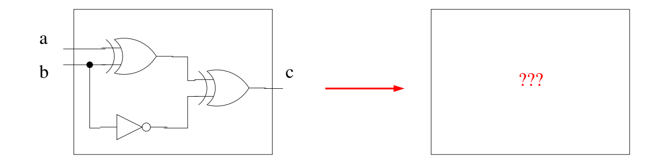
En 2012, la BBC a rapporté qu'un programme installé par la compagnie Knight Capital pour le commerce à haute fréquence en bourse, l'a fait perdre $440m en 45 minutes.
En fin des comptes, une “fonctionnalité d'arrêt de logique” aurait permis d'arrêter la folie.
Aurait-on dû analyser la “logique” du programme en amont ?

Application : Cryptomonnaie

La cryptomonnaie est une science en soi, mais au cœur se trouve une comptabilité (qui doit quelle somme à qui ?) dont on exige qu'elle soit fiable. Donc on a besoin de la cryptographie.
Des attaques spectaculaires ont été menées, par exemple en 2016 sur la monnaie Ether : quelqu'un a volé €65m.
Pour ce genre d'attaques, parfois même les assurances refusent de payer car il s'agirait "d'actes de guerre".
Grand défi de vérification !

Méthodes : Preuves d'équivalence

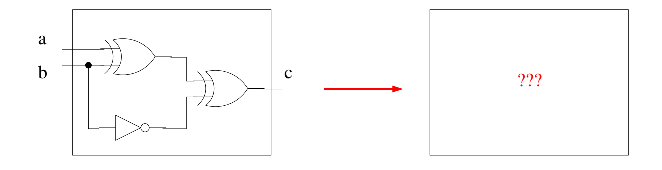
En électronique, on a des circuits comme celui-ci (sauf qu'en pratique c'est beaucoup plus compliqué que ça) :



Nous allons formaliser les circuits par des formules en logique propositionnelle ; dans ce cas : $(a \oplus b) \oplus (\neg b)$ où $\oplus$ est le "ou exclusif".

Méthodes : Preuves d'équivalence

En électronique, on a des circuits comme celui-ci (sauf qu'en pratique c'est beaucoup plus compliqué que ça) :



Nous allons formaliser les circuits par des formules en logique propositionnelle ; dans ce cas : $(a \oplus b) \oplus (\neg b)$ où $\oplus$ est le "ou exclusif".

Devoir à la maison / TD

Dessinez un circuit plus simple avec la même fonctionnalité.

Nous allons définir et prouver l'équivalence de formules.

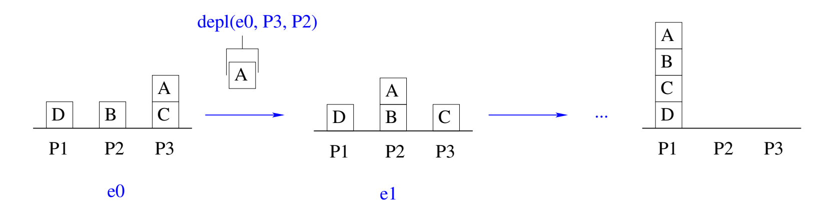


Méthodes : Systèmes à état

Robotique / Planification :

Exemple :

- Un état est caractérisé par des objets A, B, C, D empilés arbitrairement sur trois positions P_1, P_2, P_3
- Opérations : Le robot peut déplacer un seul objet au sommet d'une pile vers le sommet d'une autre pile
- But : empiler A, B, C, D (dans l'ordre) sur P_1
- Solution : séquence d'opérations qui atteignent le but



Méthodes : Systèmes à état

Modélisation :

- Prédicat ternaire `Sur` : un bloc est sur un autre bloc / sur une position dans un état
  Exemples : `Sur(D, P1, e0)` et `Sur(A, B, e1)`
- Fonction ternaire `depl` : convertir un état en déplaçant le sommet d'une position vers une autre
  Exemple : L'état `e1` est : `depl(e0, P3, P2)`

À faire :

- Décrivez entièrement l'état `e1`
- Trouvez la séquence d'opérations menant au but : les outils de logique peuvent être utiles pour cela !

Méthodes : Systèmes à état

Programmes impératifs :

- Un état est charactérisé par un ensemble de variables et de valeurs associées.
- Opérations :
  - Affectations
  - Séquences, structures de contrôle, boucles

x	5
y	10
i	5

$x = x + 3;$ →

x	8
y	10
i	5

$y = y + 2;$ →

x	8
y	12
i	5

$i = i - 1;$ → ↻ →

x	20
y	20
i	0

Méthodes : Systèmes à état

Pré- /Postconditions :

```
{ y = 2 * x ∧ x ≥ 0
} i = x; while (i >
0) { x = x + 3; y =
y + 2; i = i - 1; }
{ y = x }
```

Correction du programme :

- Est-ce que le programme transforme tout état qui satisfait la précondition en un état qui satisfait la postcondition ?
- Vérification à l'aide d'un invariant : $i \geq 0 \wedge\ y - x = i$

Résumé

La logique est essentielle dans des domaines tels que

- l'intélligence artificielle
- la sûreté de fonctionnement et la sécurité

La logique permet de décrire

- l'équivalence fonctionnelle et comportementale (exemple : circuit)
- les propriétés des systèmes de transition :
  - exemple planification :
    Donné : État initial, état final.
    But : Recherche de séquence d'actions
  - exemple programme impératif :
    Donné : Séquence d'actions (le programme)
    But : Vérification de rapport entre un état initial et un état final



Plan

Plan

Quand on parle de “la logique”, il y a (au moins) deux dimensions :

- Quelle logique : logique propositionnelle, logique des prédicats ...
- Quel aspect : syntaxe, sémantique, modélisation, méthodes de preuves ...

Plan

Quand on parle de “la logique”, il y a (au moins) deux dimensions :

- Quelle logique : logique propositionnelle, logique des prédicats . . .
- Quel aspect : syntaxe, sémantique, modélisation, méthodes de preuves . . .

Ça nous donne une “carte du terrain” :

		Lo. prop.	Lo. prédicats	. . .
Syntaxe				
Sémantique				
Modélisation				
Méth. preuve	• Déd. nat.			
	• Tableaux			
	• Résolution			

Plan

Quand on parle de “la logique”, il y a (au moins) deux dimensions :

- Quelle logique : logique propositionnelle, logique des prédicats ...
- Quel aspect : syntaxe, sémantique, modélisation, méthodes de preuves ...

Ça nous donne une “carte du terrain” :

		Lo. prop.	Lo. prédicats	...
Syntaxe		☞		
Sémantique				
Modélisation				
Méth. preuve	• Déd. nat.			
	• Tableaux			
	• Résolution			

Syntaxe, sémantique, modélisation, méthodes de preuve

- Syntaxe : à quoi ça ressemble ?
- Sémantique : qu’est-ce que ça veut dire ?
- Modélisation : comment traduire entre le français et la logique ?
- Méthodes de preuve : comment ça marche ?
  ou bien : à quoi ça sert ?



Langages logiques (1)

Les langages logiques sont :

- des abstractions du langage naturel ou mathématique :
  - Lang. nat. : “Il fait nuit, et la lumière est allumée”
  - Logique : $n \wedge l$
  - avec : $n \rightsquigarrow$ il fait nuit ; $l \rightsquigarrow$ la lumière est allumée
- …qui ne permettent pas d’exprimer certaines nuances :
  - Lang. nat. : “Il fait nuit mais la lumière est allumée”
  - Logique : $n \wedge l$
- …mais plus précis :
  - Lang. nat. : “Je suis au bureau ou je suis dans le jardin et je lis un livre”
  - Logique : $(b \vee j) \wedge l$ ou $b \vee (j \wedge l)$
  - avec : $b \rightsquigarrow$ je suis au bureau ; $j \rightsquigarrow$ je suis dans le jardin ; $l \rightsquigarrow$ je lis un livre



Langages logiques (2)

La logique des propositions LProp

- est une logique très simple
- fait une abstraction très grossière

Elle ne permet pas d'exprimer

- des rapports entre des individus :
  "entre deux nombres, il y a un troisième nombre"
  $\rightsquigarrow$ logique des prédicats
- des rapports temporels :
  "S'il fait nuit, la lumière va s'allumer"
  $\rightsquigarrow$ logiques temporelles
- des souhaits, obligations, possibilités, ... :
  "Je pense que s'il fait nuit, la lumière devrait être allumée"
  $\rightsquigarrow$ logiques modales

Abstractions de la Lprop (1)

La logique des propositions

- remplace des propositions entières par des variables propositionnelles
  il fait nuit $\rightsquigarrow$ n; la lumière est allumée $\rightsquigarrow$ l
- ...et les relie par des connecteurs logiques :
  - "Il fait nuit, et la lumière est allumée" : $n \wedge l$
  - "Il fait nuit, ou la lumière est allumée" : $n \vee l$ (sens inclusif)
  - "S'il fait nuit, alors la lumière est allumée" : $n \longrightarrow l$ (n est condition suffisante pour l)
  - "Il ne fait pas nuit" : $\neg n$

Abstractions de la Lprop (2)

Une proposition correspond à une phrase élémentaire en français :

- “Eve mange une grande pomme”
  ou simplément : “Eve mange”

mais pas à

- un substantif : “Eve”, “une pomme”
- un verbe : “mange”
- un adjectif : “grand”

Pour avoir une correspondance juste : réécrire les phrases :

- Lang. nat. : “Eve mange une pomme et un abricot”
- Logique : $p \land a$
- avec : $p \rightsquigarrow$ “Eve mange une pomme” ; $a \rightsquigarrow$ “Eve mange un abricot”
- mais pas(!) : $p \rightsquigarrow$ “Eve mange une pomme” ; $a \rightsquigarrow$ “un abricot”



Abstractions de la Lprop (3)

Inversion de l'ordre des connecteurs :

- "Je vais à la plage s'il fait beau"
  (a la même signification que "S'il fait beau, je vais à la plage")
  en logique : $b \longrightarrow p$
  avec : $b \rightsquigarrow$ il fait beau ; $p \rightsquigarrow$ je vais à la plage

Attention à l'ambiguïté du langage naturel :

- "Je vais au cinéma ou à la plage s'il fait beau"
  1. $b \longrightarrow (c \vee p)$
  2. $c \vee (b \longrightarrow p)$

Devoir à la maison / TD

Laquelle des deux formules est plus plausible dans la réalité ?

Définition formelle de la Lprop (1)

Définition inductive : Soit *PROP* un ensemble de variables propositionnelles (typiquement $\{p, q, \ldots\}$).

Définition formelle de la Lprop (1)

Définition inductive : Soit *PROP* un ensemble de variables propositionnelles (typiquement $\{p, q, \ldots\}$).
On définit l'ensemble *FORM* des formules par induction. *FORM* est le plus petit ensemble qui satisfait les conditions :

1. Variable propositionnelle : Si $p \in PROP$, alors $p \in FORM$
2. Constante "faux" : $\bot \in FORM$

Définition formelle de la Lprop (1)

Définition inductive : Soit *PROP* un ensemble de variables propositionnelles (typiquement $\{p, q, \ldots\}$).
On définit l'ensemble *FORM* des formules par induction. *FORM* est le plus petit ensemble qui satisfait les conditions :

1. Variable propositionnelle : Si $p \in PROP$, alors $p \in FORM$
2. Constante "faux" : $\bot \in FORM$
3. Négation : Si $A \in FORM$,
   alors $(\neg A) \in FORM$
4. Conjonction ("et") : Si $A \in FORM$ et $B \in FORM$,
   alors $(A \wedge B) \in FORM$
5. Disjonction ("ou") : Si $A \in FORM$ et $B \in FORM$,
   alors $(A \vee B) \in FORM$
6. Implication ("si ...alors") : Si $A \in FORM$ et $B \in FORM$,
   alors $(A \longrightarrow B) \in FORM$

(*A* et *B* représentent des formules, c.-à-d., *A* et *B* sont des métavariables).

Comprendre une définition inductive

"*FORM* est le plus petit ensemble ..." :

- $(p \bowtie q) \notin FORM$, parce qu'aucune règle ne génère $(p \bowtie q)$

Comprendre une définition inductive

"*FORM* est le plus petit ensemble ..." :

- $(p \bowtie q) \notin FORM$, parce qu'aucune règle ne génère $(p \bowtie q)$
- ☕ $\notin FORM$,

Comprendre une définition inductive

"*FORM* est le plus petit ensemble . . ." :

- $(p \bowtie q) \notin FORM$, parce qu'aucune règle ne génère $(p \bowtie q)$
- ☕ $\notin FORM$, 🚲 $\notin FORM$,

Comprendre une définition inductive

"*FORM* est le plus petit ensemble ..." :

- $(p \bowtie q) \notin FORM$, parce qu'aucune règle ne génère $(p \bowtie q)$
- ☕ $\notin FORM$, 🚲 $\notin FORM$, ⚽ $\notin FORM$, parce que ...

Comprendre une définition inductive

"*FORM* est le plus petit ensemble ..." :

- $(p \bowtie q) \notin FORM$, parce qu'aucune règle ne génère $(p \bowtie q)$
- ☕ $\notin FORM$, 🚲 $\notin FORM$, ⚽ $\notin FORM$, parce que ...

Question

Pourquoi $((p \wedge (q \vee r))) \longrightarrow (\neg s)) \notin FORM$?



Comprendre une définition inductive

"*FORM* est le plus petit ensemble . . ." :

- $(p \bowtie q) \notin FORM$, parce qu'aucune règle ne génère $(p \bowtie q)$
- ☕ $\notin FORM$, 🚲 $\notin FORM$, ⚽ $\notin FORM$, parce que . . .

Question

Pourquoi $((p \wedge (q \vee r))) \longrightarrow (\neg s)) \notin FORM$?

Quand on parle de "la formule $((A \longrightarrow B) \vee A)$", c'est dans un sens schématique. $((A \longrightarrow B) \vee A)$ n'est pas une formule concrète, mais $((A \longrightarrow B) \vee A)$ représente les formules concrètes $((p \longrightarrow q) \vee p)$, $((p \longrightarrow p) \vee p)$, $(((p \wedge q) \longrightarrow r) \vee (p \wedge q))$, etc.

Comprendre une définition inductive

"*FORM* est le plus petit ensemble . . ." :

- $(p \bowtie q) \notin FORM$, parce qu'aucune règle ne génère $(p \bowtie q)$
- ☕ $\notin FORM$, 🚲 $\notin FORM$, ⚽ $\notin FORM$, parce que . . .

Question

Pourquoi $((p \wedge (q \vee r))) \longrightarrow (\neg s)) \notin FORM$?

Quand on parle de "la formule $((A \longrightarrow B) \vee A)$", c'est dans un sens schématique. $((A \longrightarrow B) \vee A)$ n'est pas une formule concrète, mais $((A \longrightarrow B) \vee A)$ représente les formules concrètes $((p \longrightarrow q) \vee p)$, $((p \longrightarrow p) \vee p)$, $(((p \wedge q) \longrightarrow r) \vee (p \wedge q))$, etc.

Question

Écrivez 10 formules basées sur $PROP = \{p, q, r\}$.



Conventions syntaxiques (1)

On peut omettre des parenthèses selon les conventions suivantes :

- Priorité : La priorité décroissante des opérateurs est $\neg, \wedge, \vee, \longrightarrow$.
  Exemples :
  - $(A \wedge B \vee C)$ est $((A \wedge B) \vee C)$
  - $(\neg A \vee B)$ est $((\neg A) \vee B)$
  - $(A \wedge B \longrightarrow A \vee B)$ est $((A \wedge B) \longrightarrow (A \vee B))$
- Associativité : Les opérateurs binaires associent à droite :
  - $A \wedge B \wedge C$ correspond à $(A \wedge (B \wedge C))$
  - $A \longrightarrow B \longrightarrow C$ correspond à $(A \longrightarrow (B \longrightarrow C))$

  Attention : $(A \longrightarrow (B \longrightarrow C))$ et $((A \longrightarrow B) \longrightarrow C)$ ont une sémantique (à voir ultérieurement) différente !
- Enfin, on omet les parenthèses tout autour de la formule (lorsqu'elle n'est pas une variable ou $\bot$).



Conventions syntaxiques (2)

On peut introduire d'autres connecteurs comme abréviations :

- Constante "vrai" : $\top$ défini par $\neg\bot$
- Double-implication : $(A \leftrightarrow B)$ défini par $((A \longrightarrow B) \wedge (B \longrightarrow A))$
- Ou exclusif : $(A \oplus B)$ défini par $((A \vee B) \wedge (\neg(A \wedge B)))$

Le connecteur $\neg$ est parfois défini comme une abréviation : $\neg A$ défini par $A \longrightarrow \bot$.
Ça se clarifiera quand on regardera la sémantique.

Conventions syntaxiques (2)

On peut introduire d'autres connecteurs comme abréviations :

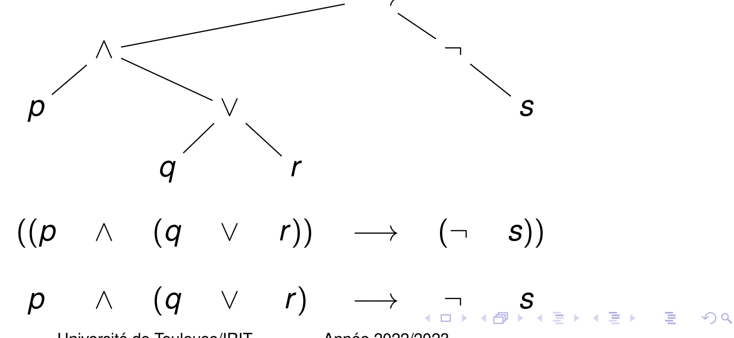
- Constante "vrai" : $\top$ défini par $\neg\bot$
- Double-implication : $(A \leftrightarrow B)$ défini par $((A \longrightarrow B) \wedge (B \longrightarrow A))$
- Ou exclusif : $(A \oplus B)$ défini par $((A \vee B) \wedge (\neg(A \wedge B)))$

Le connecteur $\neg$ est parfois défini comme une abréviation : $\neg A$ défini par $A \longrightarrow \bot$.
Ça se clarifiera quand on regardera la sémantique.
Ici, les méta-variables A, B, C,... représentent des formules

Arbres syntaxiques (1)

Plusieurs représentations de la même formule :

- Arbre syntaxique
- Représentation textuelle : parenthésage maximal (selon la définition inductive de *FORM*)
- Représentation textuelle : parenthésage minimal (selon les règles sur la diapo 52)



Astuce pour le parenthésage maximal

On voit bien que la définition de *FORM* fait qu'une paire de parenthèses est ajoutée avec chacun des connecteurs pour négation, conjonction, disjonction et implication. Ainsi, une formule qui a n connecteurs doit forcément contenir n paires de parenthèses en parenthésage maximal.

Compter les parenthèses et les connecteurs peut alors aider avec la tâche d'identifier une formule qui n'est pas en parenthésage maximal.

Exercices

Question

- Mettre en parenthésage minimal la formule suivante : $((((p \vee q) \longrightarrow r) \wedge ((p \vee q) \wedge (s \longrightarrow (\neg r)))) \longrightarrow (\neg s))$
- Mettre en parenthésage maximal la formule suivante : $\neg(p \longrightarrow \neg p \wedge q) \wedge q \longrightarrow \neg r$
- Tracez les arbres syntaxiques de ces 2 formules

Devoir à la maison / TD

- Mettre en parenthésage minimal la formule suivante : $(((s \longrightarrow (p \vee q)) \wedge (\neg s)) \wedge ((\neg q) \longrightarrow (r \wedge (t \longrightarrow (\neg q)))))$
- Mettre en parenthésage maximal la formule suivante : $p \longrightarrow q \wedge s \vee p \longrightarrow \neg q \wedge s$
- Tracez les arbres syntaxiques de ces 2 formules



Résumé

Syntaxe de la logique des propositions

- Rapport avec le langage naturel
- Variables propositionnelles, connecteurs
- Différentes représentations : textuelle, arborescente

Plan

		Lo. prop.	Lo. prédicats	. . .
Syntaxe		✔		
Sémantique				
Modélisation		☞		
Méth. preuve	• Déd. nat.			
	• Tableaux			
	• Résolution			

Exercice de modélisation : Morpion

Devoir à la maison / TD

Modélisez le jeu de morpion en logique propositionnelle :

- Quelles variables faut-il ?
- Comment peut-on décrire des configurations comme : “le joueur ○ gagne avec la première ligne” ?

Modélisation en logique propositionnelle : Principes

- Chaque variable doit absolument correspondre à une proposition, à une phrase. Donc on ne peut pas avoir une variable qui représente "croix", ou qui représente "la case (1,1)", car "croix" n'est pas une phrase.
- Cette phrase doit être atomique, c.-à-d., indivisible. Par exemple, "le joueur croix gagne" n'est pas atomique car ça se décompose en "il y a une croix sur la case A1 et ..., ou ...".
- La phrase doit aussi être indépendante. Par exemple "Cette case est remplie par une croix" parle d'une case qui a dû être mentionnée auparavant ; cela n'est pas possible.
- Il faut bien profiter de la possibilité d'exprimer une phrase comme négation d'une autre phrase : donc si vous avez une variable $C11$ pour dire "il y a une croix sur la case (1,1)" et une variable $R11$ pour dire "il y a un rond sur la case (1,1)", inutile d'avoir une variable pour "la case (1,1) est vide" car ça s'exprime comme $\neg C11 \wedge \neg R11$.

Modélisation en logique propositionnelle : Principes (2)

- Il faut parfois “lire entre les lignes” mais quand même prendre le texte le plus à la lettre possible.
- Si on a le choix, il faut préférer le simple : Rasoir d’Ockham
- Il y a presque toujours plusieurs manières de faire.

Modélisation en logique propositionnelle : Principes (2)

- Il faut parfois “lire entre les lignes” mais quand même prendre le texte le plus à la lettre possible.
- Si on a le choix, il faut préférer le simple : Rasoir d’Ockham
- Il y a presque toujours plusieurs manières de faire.
- Le plus important : Quelques uns de ces principes ne s’appliquent qu’à la logique propositionnelle ; pour d’autres logiques, les principes sont différents !

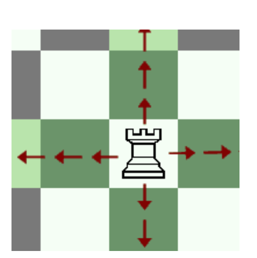
Sachez en plus qu’en pratique les problèmes seront évidemment beaucoup plus grands que les exemples présentés ici.



Exercice de modélisation : Mini-échecs

On considère un fragment du jeu d'échecs, avec une illustration des déplacements possibles de la tour :

A1	A2	A3
B1	B2	B3
C1	C2	C3



Exercice de modélisation : Mini-échecs (2)

1. Introduisez des variables propositionnelles pour représenter la présence d'une tour blanche ou d'un pion noir sur chaque case du mini-échiquier.

Exercice de modélisation : Mini-échecs (2)

1. Introduisez des variables propositionnelles pour représenter la présence d'une tour blanche ou d'un pion noir sur chaque case du mini-échiquier.
   $TBA1$: “Il y a une tour blanche sur la case A1.”
   $\ldots$
   $TBC3$: “Il y a une tour blanche sur la case C3.”
   $PNA1$: “Il y a un pion noir sur la case A1.”
   $\ldots$
   $PNC3$: “Il y a un pion noir sur la case C3.”

Exercice de modélisation : Mini-échecs (2)

1. Introduisez des variables propositionnelles pour représenter la présence d'une tour blanche ou d'un pion noir sur chaque case du mini-échiquier.
   $TBA1$: "Il y a une tour blanche sur la case A1."
   $\ldots$
   $TBC3$: "Il y a une tour blanche sur la case C3."
   $PNA1$: "Il y a un pion noir sur la case A1."
   $\ldots$
   $PNC3$: "Il y a un pion noir sur la case C3."
2. Écrivez une formule propositionnelle disant "il y a au moins une tour blanche sur le mini-échiquier".

Exercice de modélisation : Mini-échecs (2)

1. Introduisez des variables propositionnelles pour représenter la présence d'une tour blanche ou d'un pion noir sur chaque case du mini-échiquier.
   $TBA1$: "Il y a une tour blanche sur la case A1."
   ...
   $TBC3$: "Il y a une tour blanche sur la case C3."
   $PNA1$: "Il y a un pion noir sur la case A1."
   ...
   $PNC3$: "Il y a un pion noir sur la case C3."
2. Écrivez une formule propositionnelle disant "il y a au moins une tour blanche sur le mini-échiquier".

$$TBA1 \vee TBA2 \vee \ldots \vee TBC3$$



Exercice de modélisation : Mini-échecs (3)

1. Écrivez une formule propositionnelle disant “aucune tour blanche ne menace aucun pion noir”.

Exercice de modélisation : Mini-échecs (3)

1. Écrivez une formule propositionnelle disant “aucune tour blanche ne menace aucun pion noir”.

$$(TBA1 \longrightarrow \neg PNA2 \wedge \neg PNA3 \wedge \neg PNB1 \wedge \neg PNC1)$$
$$(TBA2 \longrightarrow \neg PNA1 \wedge \neg PNA3 \wedge \neg PNB2 \wedge \neg PNC2)$$
$$\ldots$$
$$(TBC3 \longrightarrow \neg PNC1 \wedge \neg PNC2 \wedge \neg PNA3 \wedge \neg PNB3)$$

Exercice de modélisation : Mini-échecs (3)

1. Écrivez une formule propositionnelle disant “aucune tour blanche ne menace aucun pion noir”.

$$(TBA1 \longrightarrow \neg PNA2 \wedge \neg PNA3 \wedge \neg PNB1 \wedge \neg PNC1)$$
$$(TBA2 \longrightarrow \neg PNA1 \wedge \neg PNA3 \wedge \neg PNB2 \wedge \neg PNC2)$$
$$\ldots$$
$$(TBC3 \longrightarrow \neg PNC1 \wedge \neg PNC2 \wedge \neg PNA3 \wedge \neg PNB3)$$

À débattre : si la tour et le pion se trouvaient sur la même case (ce qui n’existe pas dans le vrai jeu), est-ce que la tour “menacerait” le pion ? Si vous pensez que oui, votre formalisation devrait ressembler à cela :

$$(TBA1 \longrightarrow \neg PNA1 \wedge \neg PNA2 \wedge \neg PNA3 \wedge \neg PNB1 \wedge \neg PNC1)$$
$$(TBA2 \longrightarrow \neg PNA2 \wedge \neg PNA1 \wedge \neg PNA3 \wedge \neg PNB2 \wedge \neg PNC2)$$
$$\ldots$$
$$(TBC3 \longrightarrow \neg PNC3 \wedge \neg PNC1 \wedge \neg PNC2 \wedge \neg PNA3 \wedge \neg PNB3)$$

Exercice de modélisation : Histoire policière

“Un vol a été commis, on a relevé des traces de chaussures taille 40 et le voleur a été aperçu : il est petit. Parmi les 3 suspects (A, B et C), A est grand et chausse du 40, B est petit et chausse du 45, enfin C est petit et chausse du 40.”

Quelles variables introduire ?

Exercice de modélisation : Histoire policière

“Un vol a été commis, on a relevé des traces de chaussures taille 40 et le voleur a été aperçu : il est petit. Parmi les 3 suspects (A, B et C), A est grand et chausse du 40, B est petit et chausse du 45, enfin C est petit et chausse du 40.”
Quelles variables introduire ?

- L’ histoire parle d’exactement trois personnes et d’un vol, il est donc parfaitement raisonnable de lire entre les lignes que le voleur est une de ces personnes. On aura donc des variables Av, Bv, Cv pour dire que “A est le voleur” etc. Si l’exercice s’annonce “formalisez cette histoire”, cette formalisation devrait certainement contenir la formule $Av \lor Bv \lor Cv$.
- Les personnes peuvent être grandes ou petites, donc on aura des variables Ag, Bg, Cg pour dire “A est grand” etc., et on est petit ssi on n’est pas grand.

Exercice de modélisation : Histoire policière (2)

- Les personnes peuvent chausser 40 ou 45, donc on aura des variables $Ac45$, $Bc45$, $Cc45$ pour dire “A chausse du 45” etc., et on chausse du 40 ssi on ne chausse pas du 45.

Exercice de modélisation : Histoire policière (2)

- Les personnes peuvent chausser 40 ou 45, donc on aura des variables $Ac45$, $Bc45$, $Cc45$ pour dire “A chausse du 45” etc., et on chausse du 40 ssi on ne chausse pas du 45.
- Est-ce que “chausser du n” et “porter des chaussures de pointure n” est la même chose ? Ça se discute ! Il vaudrait probablement mieux distinguer entre les deux (introduire $Ap45$, $Bp45$, $Cp45$), et la formalisation devrait contenir la formule

$$(Ac45 \longrightarrow Ap45) \wedge (Bc45 \longrightarrow Bp45) \wedge (Cc45 \longrightarrow Cp45)$$

car on ne peut raisonnablement pas porter du 40 si on chausse du 45 (mais à la rigueur vice versa).



Plan

Plan

		Lo. prop.	Lo. prédicats	...
Syntaxe		✔		
Sémantique		☞		
Modélisation		✔		
Méth. preuve	• Déd. nat.			
	• Tableaux			
	• Résolution			

Problématique

Vu jusqu'à maintenant : la structure du langage logique : Syntaxe (grec : syn-taxis : composition)
Dans cette section : la signification du langage logique : Sémantique (grec : sema : signe)

Dichotomie syntaxe / sémantique dans tout langage :

- en logique et dans les langages de programmation
- en linguistique (signifiant/signifié $\sim$ le mot/la chose)

Problématique

Vu jusqu'à maintenant : la structure du langage logique : Syntaxe (grec : syn-taxis : composition)
Dans cette section : la signification du langage logique : Sémantique (grec : sema : signe)

Dichotomie syntaxe / sémantique dans tout langage :

- en logique et dans les langages de programmation
- en linguistique (signifiant/signifié $\sim$ le mot/la chose)

On va maintenant précisément répondre à la question : quand est-ce qu'une formule est vraie ($= 1$) ou fausse ($= 0$) ?

Valuation

- En général, une formule propositionnelle n'est ni vraie ni fausse a priori. Cela dépend des variables de la formule.

Valuation

- En général, une formule propositionnelle n'est ni vraie ni fausse a priori. Cela dépend des variables de la formule.
- De la même façon, une équation (par exemple $x^2 + 1 = y$) n'est ni vraie ni fausse tant qu'on ne connaît pas les valeurs de x et de y, c'est-à-dire le contexte.
- Si le contexte associe à x la valeur 2, et à y la valeur 5, alors elle est vraie, dans d'autres contextes elle serait fausse.

Valuation

- En général, une formule propositionnelle n'est ni vraie ni fausse a priori. Cela dépend des variables de la formule.
- De la même façon, une équation (par exemple $x^2 + 1 = y$) n'est ni vraie ni fausse tant qu'on ne connaît pas les valeurs de x et de y, c'est-à-dire le contexte.
- Si le contexte associe à x la valeur 2, et à y la valeur 5, alors elle est vraie, dans d'autres contextes elle serait fausse.
- Réciproquement, on peut se demander quel sont les contextes qui la rendent vraies (=quelles en sont les solutions).

Valuation

- En général, une formule propositionnelle n'est ni vraie ni fausse a priori. Cela dépend des variables de la formule.
- De la même façon, une équation (par exemple $x^2 + 1 = y$) n'est ni vraie ni fausse tant qu'on ne connaît pas les valeurs de x et de y, c'est-à-dire le contexte.
- Si le contexte associe à x la valeur 2, et à y la valeur 5, alors elle est vraie, dans d'autres contextes elle serait fausse.
- Réciproquement, on peut se demander quel sont les contextes qui la rendent vraies (=quelles en sont les solutions).
- Les mêmes questions se posent quant à la vérité/fausseté des formules logiques...

Valuation (2)

- Les contextes possibles pour une formule logique s'appellent des valuations
- Elles décrivent quelle valeur de vérité est associée à chaque variable propositionnelle

Valuation (2)

- Les contextes possibles pour une formule logique s'appellent des valuations
- Elles décrivent quelle valeur de vérité est associée à chaque variable propositionnelle
- Formellement : une valuation est une fonction $v : PROP \Rightarrow \{0, 1\}$
- Arbitrairement on pose : $v(p) = 0$: "p faux" ; $v(p) = 1$: "p vrai" ;

Interprétation

Chaque valuation peut être étendue de *PROP* à *FORM* de la manière suivante :

1. (Variable) : $I_v(p) = v(p)$
2. (Constante) : $I_v(\bot) = 0$
3. (Négation) : $I_v(\neg A) = 1 - I_v(A)$
4. (Conjonction) : $I_v(A \wedge B) = min(I_v(A), I_v(B))$
5. (Disjonction) : $I_v(A \vee B) = max(I_v(A), I_v(B))$
6. (Implication) : $I_v(A \longrightarrow B) = max(1 - I_v(A), I_v(B))$ (discussion plus loin)

C'est une définition récursive.
On parle alors d'une interprétation.



Signature de I

Dans les mathématiques, il est habituel de spécifier pour une fonction sa signature, c.-à-d., quelles sont les possibles entrées et quels sont les possibles résultats, par exemple : $+ : \mathbb{N} \Rightarrow \mathbb{N} \Rightarrow \mathbb{N}$.
Quelle est la signature de I ?

Signature de I

Dans les mathématiques, il est habituel de spécifier pour une fonction sa signature, c.-à-d., quelles sont les possibles entrées et quels sont les possibles résultats, par exemple : $+ : \mathbb{N} \Rightarrow \mathbb{N} \Rightarrow \mathbb{N}$.
Quelle est la signature de I ?
La notation $I_v(\bot)$, $I_v(\neg A)$, ... nous dit que I est appliquée à deux arguments, une valuation (signature $PROP \Rightarrow \{0,1\}$) et une formule, la signature de I doit donc être $(PROP \Rightarrow \{0,1\}) \Rightarrow FORM \Rightarrow \dots$.

Signature de I

Dans les mathématiques, il est habituel de spécifier pour une fonction sa signature, c.-à-d., quelles sont les possibles entrées et quels sont les possibles résultats, par exemple : $+ : \mathbb{N} \Rightarrow \mathbb{N} \Rightarrow \mathbb{N}$.
Quelle est la signature de I ?
La notation $I_v(\bot)$, $I_v(\neg A)$, ... nous dit que I est appliquée à deux arguments, une valuation (signature $PROP \Rightarrow \{0, 1\}$) et une formule, la signature de I doit donc être $(PROP \Rightarrow \{0, 1\}) \Rightarrow FORM \Rightarrow \ldots$.
Dans l'égalité $I_v(p) = v(p)$ on voit que le résultat est comme pour v, donc dans $\{0, 1\}$. La signature de I est donc
$(PROP \Rightarrow \{0, 1\}) \Rightarrow FORM \Rightarrow \{0, 1\}$. L'utilisation d'un index pour v donne l'intuition "v n'est qu'un petit détail, l'argument important est la formule" ou bien "on fixe d'abord v et après on regarde ce que signifie la formule".

Signature de I

Dans les mathématiques, il est habituel de spécifier pour une fonction sa signature, c.-à-d., quelles sont les possibles entrées et quels sont les possibles résultats, par exemple : $+ : \mathbb{N} \Rightarrow \mathbb{N} \Rightarrow \mathbb{N}$.
Quelle est la signature de I ?
La notation $I_v(\bot)$, $I_v(\neg A)$, ... nous dit que I est appliquée à deux arguments, une valuation (signature $PROP \Rightarrow \{0, 1\}$) et une formule, la signature de I doit donc être $(PROP \Rightarrow \{0, 1\}) \Rightarrow FORM \Rightarrow \ldots$.
Dans l'égalité $I_v(p) = v(p)$ on voit que le résultat est comme pour v, donc dans $\{0, 1\}$. La signature de I est donc
$(PROP \Rightarrow \{0, 1\}) \Rightarrow FORM \Rightarrow \{0, 1\}$. L'utilisation d'un index pour v donne l'intuition "v n'est qu'un petit détail, l'argument important est la formule" ou bien "on fixe d'abord v et après on regarde ce que signifie la formule".
Si on écrit la signature comme $(PROP \Rightarrow \{0, 1\}) \Rightarrow (FORM \Rightarrow \{0, 1\})$, ça ne change rien formellement, mais donne l'intuition "une interprétation est une extension d'une valuation".

Nombre de valuations

Rappel : une valuation est une fonction $v : PROP \Rightarrow \{0, 1\}$.

Question

Combien de valuations y a-t-il ?



Nombre de valuations

Rappel : une valuation est une fonction $v : PROP \Rightarrow \{0, 1\}$.

Question

Combien de valuations y a-t-il ?

$$2^{\#PROP}$$

Interprétations et tables de vérité

Table de vérité (TdV) des connecteurs :

A	B	$A \wedge B$	$A \vee B$	$A \longrightarrow B$	$A \leftrightarrow B$	$A \oplus B$
0	0	0	0	1	1	0
0	1	0	1	1	0	1
1	0	0	1	0	0	1
1	1	1	1	1	1	0

La table de vérité recense toutes les valuations possibles.
Chaque ligne de la TdV correspond à une valuation. Il y en a $2^2 = 4$.

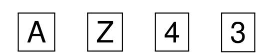
TdV de l'implication : discussion

Dans un jeu, il y a des cartes avec une lettre sur une face et un nombre sur l'autre. À un certain moment du jeu, si un joueur pose une carte avec une voyelle sur une face, cette carte doit avoir un nombre pair sur l'autre face.
Vous voyez les cartes suivantes, lesquelles faut-il retourner pour vérifier que ce sont des cartes autorisées ?

A Z 4 3

TdV de l'implication : discussion

Dans un jeu, il y a des cartes avec une lettre sur une face et un nombre sur l'autre. À un certain moment du jeu, si un joueur pose une carte avec une voyelle sur une face, cette carte doit avoir un nombre pair sur l'autre face.
Vous voyez les cartes suivantes, lesquelles faut-il retourner pour vérifier que ce sont des cartes autorisées ?



Avant de répondre, voici un deuxième exemple, identique mais plus concret.

TdV de l'implication : discussion (2)

Dans un bar, il est interdit de servir de l'alcool à un mineur (alcool$\longrightarrow$ majeur), cette loi est respectée dans un contexte donné si la formule en bleu est vraie : être majeur est une condition nécessaire pour y boire de l'alcool. Vous voyez les commandes suivantes, sur une face il y a la boisson commandée et sur l'autre l'âge du client.

Bière	Café	21 ans	13 ans

Question

Lesquelles faut-il retourner pour vérifier que ce sont des commandes autorisées ?

TdV de l'implication : discussion (3)

Quels sont les contextes qui enfreignent la loi, ou, dit autrement, pour quelles valuations l'implication (alcool$\longrightarrow$ majeur) est-elle fausse ?

alcool	majeur	alcool $\longrightarrow$ majeur
0	0	?
0	1	?
1	0	?
1	1	?

TdV de l'implication : discussion (3)

Quels sont les contextes qui enfreignent la loi, ou, dit autrement, pour quelles valuations l'implication (alcool$\longrightarrow$ majeur) est-elle fausse ?

alcool	majeur	alcool $\longrightarrow$ majeur
0	0	?
0	1	?
1	0	?
1	1	?

On voit bien que si v(alcool)=0, la règle ne peut pas avoir été enfreinte et que si v(majeur)=1 non plus...
Le seul cas où elle l'est est quand v(alcool)=1 ET que v(majeur)=0 !

Interprétations et tables de vérité

TdV de $(p \wedge q) \vee (\neg r)$

p	q	r	$p \wedge q$	$\neg r$	$(p \wedge q) \vee (\neg r)$
0	0	0	0	1	1
0	0	1	0	0	0
0	1	0	0	1	1
0	1	1	0	0	0
1	0	0	0	1	1
1	0	1	0	0	0
1	1	0	1	1	1
1	1	1	1	0	1

La table de vérité à 2^n lignes et recense toutes les valuations possibles pour n variables propositionnelles.
Chaque ligne de la TdV correspond à une valuation.

Interprétations et tables de vérité

TdV de $(p \wedge q) \vee (\neg r)$

p	q	r	$p \wedge q$	$\neg r$	$(p \wedge q) \vee (\neg r)$
0	0	0	0	1	1
0	0	1	0	0	0
0	1	0	0	1	1
0	1	1	0	0	0
1	0	0	0	1	1
1	0	1	0	0	0
1	1	0	1	1	1
1	1	1	1	0	1

Exemple : valuation v avec : $v(p) = 1, v(q) = 0, v(r) = 0$
$I_v((p \wedge q) \vee (\neg r)) = max(I_v(p \wedge q), I_v(\neg r)) = max(min(I_v(p), I_v(q)), 1 - I_v(r)) = max(min(1, 0), 1 - 0) = max(0, 1) = 1$

Interprétations et tables de vérité

Considérons un sommaire de 3 tables de vérités :

p	q	r	$p \wedge q \longrightarrow q \vee r$	$p \vee q \longrightarrow \neg p \wedge \neg q$	$(p \wedge q) \vee (\neg r)$
0	0	0	1	1	1
0	0	1	1	1	0
0	1	0	1	0	1
0	1	1	1	0	0
1	0	0	1	0	1
1	0	1	1	0	0
1	1	0	1	0	1
1	1	1	1	0	1

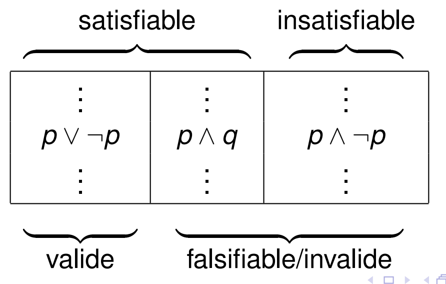
On étudiera dans la suite les différents cas . . .



Validité etc.

Définition : Une formule A est ...

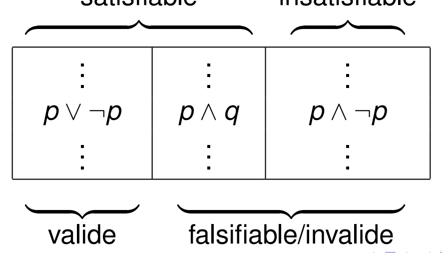
- valide (une tautologie) si, pour toute valuation v, on a $I_v(A) = 1$
- satisfiable s'il existe une valuation v telle que $I_v(A) = 1$
- insatisfiable s'il n'existe pas de valuation v telle que $I_v(A) = 1$
- falsifiable (invalide) s'il existe une valuation v telle que $I_v(A) = 0$



Validité etc.

Définition : Une formule A est ...

- valide (une tautologie) si, pour toute valuation v, on a $I_v(A) = 1$ (que des 1 dans sa TdV)
- satisfiable s'il existe une valuation v telle que $I_v(A) = 1$ (au moins un 1 dans sa TdV)
- insatisfiable s'il n'existe pas de valuation v telle que $I_v(A) = 1$ (que des 0 dans sa TdV)
- falsifiable (invalide) s'il existe une valuation v telle que $I_v(A) = 0$ (au moins un 0).



Exercices

Question

Déterminez si ces formules sont valides etc. grâce à leurs tables de vérité :

1. $(p \wedge q) \longrightarrow p$
2. $(p \longrightarrow r) \longrightarrow (p \vee q \longrightarrow r)$

Devoir à la maison / TD

Déterminez si cette formule est valide etc. grâce à sa table de vérité :
$(p \wedge (q \longrightarrow r)) \longrightarrow ((\neg p \vee q) \longrightarrow (p \wedge r))$

Exercices

Question

Déterminez si ces formules sont valides etc. grâce à leurs tables de vérité :

1. $(p \land q) \longrightarrow p$
2. $(p \longrightarrow r) \longrightarrow (p \lor q \longrightarrow r)$

Devoir à la maison / TD

Déterminez si cette formule est valide etc. grâce à sa table de vérité :
$(p \land (q \longrightarrow r)) \longrightarrow ((\neg p \lor q) \longrightarrow (p \land r))$

Rapports entre ces notions :

Devoir à la maison / TD

- Si A est valide, qu'est-ce que vous savez de $\neg A$?
- Si A est satisfiable, est-ce que $\neg A$ est insatisfiable ?

Modèles

Modèle d'une formule : Une valuation v est

- un modèle d'une formule A si $I_v(A) = 1$
  On dit : v satisfait A
  Ex. : pour $v(p) = 0, v(q) = 1$, v est un modèle de $p \vee q$
- un contre-modèle d'une formule A si $I_v(A) = 0$
  On dit : v falsifie A
  Ex. : pour $v(p) = 0, v(q) = 1$, v est un contre-modèle de $p \wedge q$

Modèles

Modèle d'un ensemble de formules : Une valuation v est

- un modèle d'un ensemble H si $I_v(A) = 1$ pour tout $A \in H$
  Ex. : pour $v(p) = 0, v(q) = 1$, v est un modèle de $\{p \vee q, q\}$
- un contre-modèle d'un ensemble H si $I_v(A) = 0$ pour au moins un $A \in H$
  Ex. : pour $v(p) = 0, v(q) = 1$, v est un contre-modèle de $\{p \vee q, p\}$

Conséquence (1)

Motivation : En mathématiques / informatique, on tire des conclusions à partir d'un ensemble d'hypothèses.

Exemple :

- H_1 : La fonction f est monotone
- H_2 : La fonction g est monotone
- C : La fonction $f \circ g$ est monotone

Conséquence (1)

Motivation : En mathématiques / informatique, on tire des conclusions à partir d'un ensemble d'hypothèses.

Exemple :

- H_1 : La fonction f est monotone
- H_2 : La fonction g est monotone
- C : La fonction $f \circ g$ est monotone

Définition : Soient $H_1, \ldots, H_n, C \in FORM$.
On dit que C est une conséquence (logique) de $H_1, \ldots, H_n$, écrit $\{H_1, \ldots, H_n\} \models C$, ssi tout modèle de $\{H_1, \ldots, H_n\}$ est aussi un modèle de C.

Cas particulier : On écrit $\models C$ au lieu de $\{\} \models C$ (c.-à-d., C est valide).

Conséquence (2)

p	q	r	$p \wedge q$	$\neg r$	$(p \wedge q) \vee (\neg r)$
0	0	0	0	1	1
0	0	1	0	0	0
0	1	0	0	1	1
0	1	1	0	0	0
1	0	0	0	1	1
1	0	1	0	0	0
1	1	0	1	1	1
1	1	1	1	0	1

Ici, on peut observer que $p, \neg r \models (p \wedge q) \vee (\neg r)$: chaque fois que toutes les hypothèses sont vérifiées, la conclusion l'est aussi.

Exercices

Question

Vrai ou faux ?

- $\{p, q\} \models p \vee q$
- $\{p, q\} \models p \wedge q$
- $\{p, q\} \models p \longrightarrow q$
- $\{p \longrightarrow q, q\} \models p$
- $\{p \longrightarrow q, p\} \models q$
- $\{p \longrightarrow q, \neg q\} \models \neg p$

Vérifiez

- si $\{A, B\} \models X$ alors $\{A, B, C\} \models X$
- $\{A, B\} \models X$ ssi $\{B, A\} \models X$
- $\{A, B\} \models X$ ssi $\{A\} \models B \longrightarrow X$

Devoir à la maison / TD

$\{A, B\} \models \perp$ ssi $\{A\} \models \neg B$

Équivalence

Deux formules A et B sont équivalentes ssi elles ont les mêmes modèles. Elles sont vraies ou fausses dans les mêmes contextes.
Notation : $A \equiv B$
Autrement dit, $A \equiv B$ ssi A et B ont les mêmes TDV.
Attention : $p \land \neg p \equiv \bot$ – il faut dresser la TDV pour $\bot$ avec la variable p qui est dans $PROP$.

Équivalence

Deux formules A et B sont équivalentes ssi elles ont les mêmes modèles. Elles sont vraies ou fausses dans les mêmes contextes.

Notation : $A \equiv B$

Autrement dit, $A \equiv B$ ssi A et B ont les mêmes TDV.

Attention : $p \wedge \neg p \equiv \bot$ – il faut dresser la TDV pour $\bot$ avec la variable p qui est dans $PROP$.

Question

- Montrer que $p \wedge q \equiv q \wedge p$
- Montrer que $p \longrightarrow q \not\equiv q \longrightarrow p$
- Montrer que $\neg p \equiv p \longrightarrow \bot$

Équivalence

Deux formules A et B sont équivalentes ssi elles ont les mêmes modèles. Elles sont vraies ou fausses dans les mêmes contextes.
Notation : $A \equiv B$
Autrement dit, $A \equiv B$ ssi A et B ont les mêmes TDV.
Attention : $p \wedge \neg p \equiv \perp$ – il faut dresser la TDV pour $\perp$ avec la variable p qui est dans $PROP$.

Question

- Montrer que $p \wedge q \equiv q \wedge p$
- Montrer que $p \longrightarrow q \not\equiv q \longrightarrow p$
- Montrer que $\neg p \equiv p \longrightarrow \perp$

Méta-langage : $\models$ et $\equiv$ ne sont pas des constructeurs de formules !
Interdit : “formules” comme $(A \models B) \equiv (A \longrightarrow B)$

Classes d'équivalence

Combien de classes d'équivalence y a-t-il ? Autrement dit, combien de formules sémantiquement différentes peut il y avoir ?

Classes d'équivalence

Combien de classes d'équivalence y a-t-il ? Autrement dit, combien de formules sémantiquement différentes peut il y avoir ?
Il y a $2^{\#PROP}$ valuations. Pour chaque valuation, l'interprétation de la formule peut être 0 ou 1, donc il y a $2^{2^{\#PROP}}$ possibilités, c.-à-d. classes d'équivalences. C'est beaucoup : $2^{2^1} = 4$, $2^{2^2} = 16$, $2^{2^3} = 256$, $2^{2^4} = 65536$, $2^{2^5} = 4294967296$, $2^{2^6} = 18446744073709551616 \ldots$!

Classes d'équivalence

Combien de classes d'équivalence y a-t-il ? Autrement dit, combien de formules sémantiquement différentes peut il y avoir ?
Il y a $2^{\#PROP}$ valuations. Pour chaque valuation, l'interprétation de la formule peut être 0 ou 1, donc il y a $2^{2^{\#PROP}}$ possibilités, c.-à-d. classes d'équivalences. C'est beaucoup : $2^{2^1} = 4$, $2^{2^2} = 16$, $2^{2^3} = 256$, $2^{2^4} = 65536$, $2^{2^5} = 4294967296$, $2^{2^6} = 18446744073709551616 \ldots$!

Question

Pour $PROP = \{p\}$, donner un représentant de chacune des 4 classes.
Pour $PROP = \{p, q\}$, donner un représentant de chacune des 16 classes.

Équivalences remarquables

Rappel : $\top :\equiv \neg\bot$

$\neg(A \vee B) \equiv \neg A \wedge \neg B$	$A \vee \top \equiv \top$	$A \vee \bot \equiv A$	$A \vee A \equiv A$
$\neg(A \wedge B) \equiv \neg A \vee \neg B$	$A \wedge \bot \equiv \bot$	$A \wedge \top \equiv A$	$A \wedge A \equiv A$
$A \vee B \equiv B \vee A$	$A \longrightarrow \top \equiv \top$	$\bot \longrightarrow A \equiv \top$	$A \vee \neg A \equiv \top$
$A \wedge B \equiv B \wedge A$	$A \longrightarrow \bot \equiv \neg A$	$\top \longrightarrow A \equiv A$	$A \wedge \neg A \equiv \bot$
$A \longrightarrow B \equiv \neg A \vee B$			
$\neg\neg A \equiv A$			

$(A \wedge B) \wedge C \equiv A \wedge (B \wedge C)$	$A \wedge (B \vee C) \equiv A \wedge B \vee A \wedge C$
$(A \vee B) \vee C \equiv A \vee (B \vee C)$	$A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$

La relation $\equiv$ est une congruence



Exercices (30')

Question

1. En utilisant les équivalences ci-dessus, vérifiez la suivante : $(A \wedge B) \longrightarrow C \equiv A \longrightarrow (B \longrightarrow C)$
2. Exprimez le nouveau connecteur $!(A, B, C)$ signifiant exactement une formule vraie sur trois
3. Exprimez les autres connecteurs uniquement à l'aide de $\neg$ et ! en fournissant des formules équivalentes

Résumé

- Différence syntaxe / sémantique
- On définit la sémantique d'une formule à l'aide d'une fonction d'interprétation
- Correspondance entre interprétations et tables de vérité
- Modèles d'une formule
- Validité, satisfiabilité
- Conséquence, équivalence logique

Plan

1. Motivation
2. Logique des propositions
   - Syntaxe (langage)
   - Modélisation
   - Sémantique (théorie des modèles)
   - Fonctions booléennes
   - Méthode de preuve : déduction naturelle
   - Induction
   - Substitutions
3. Logique du premier ordre

Fonctions booléennes

- La théorie des fonctions booléennes (théorie des circuits) est une théorie importante dans l'informatique (et pour passer un concours, apparemment).
- Cette théorie ressemble beaucoup à la logique propositionnelle mais la notation, la terminologie et le point de vue diffèrent.
- Comment les fonctions booléennes se situent dans notre “carte de terrain” ?
  - On pourrait dire : C'est une digression, ça sort de notre carte de terrain, . . .
  - . . . mais mieux vaut dire : on part de la sémantique et on va vers la syntaxe.

Référence : livre de Pierre Marchand.



Plan

		Lo. prop.	Lo. prédicats	...
Syntaxe		✔☞		
Sémantique		✔☞		
Modélisation		✔		
Méth. preuve	• Déd. nat.			
	• Tableaux			
	• Résolution			

Fonction booléenne : définition

Soit $\mathbf{B} = \{0, 1\}$.
Une fonction booléenne à n variables est une fonction $f : \mathbf{B}^n \Rightarrow \mathbf{B}$.

Fonction booléenne : définition

Soit $\mathbf{B} = \{0, 1\}$.
Une fonction booléenne à n variables est une fonction $f : \mathbf{B}^n \Rightarrow \mathbf{B}$.
Exemples :
$f = \{0 \mapsto 0, 1 \mapsto 0\}$ est une fonction booléenne à 1 variable.
$f = \{(0,0) \mapsto 0, (0,1) \mapsto 0, (1,0) \mapsto 0, (1,1) \mapsto 1\}$ est une fonction booléenne à 2 variables.
$f = \{(0,0,0) \mapsto 1, (0,0,1) \mapsto 1, (0,1,0) \mapsto 1, (0,1,1) \mapsto 1, (1,0,0) \mapsto 1, (1,0,1) \mapsto 1, (1,1,0) \mapsto 1, (1,1,1) \mapsto 1\}$ est une fonction booléenne à 3 variables.

Nombre de fonctions booléennes

L'ensemble $\mathbf{B}^n$ a 2^n éléments. Pour chaque élément, le résultat de f peut être 0 ou 1, donc il y a 2^{2^n} fonctions booléennes. C'est beaucoup : $2^{2^1} = 4$, $2^{2^2} = 16$, $2^{2^3} = 256$, $2^{2^4} = 65536$, $2^{2^5} = 4294967296$, $2^{2^6} = 18446744073709551616 \ldots$!

Nombre de fonctions booléennes

L'ensemble $\mathbf{B}^n$ a 2^n éléments. Pour chaque élément, le résultat de f peut être 0 ou 1, donc il y a 2^{2^n} fonctions booléennes. C'est beaucoup : $2^{2^1} = 4$, $2^{2^2} = 16$, $2^{2^3} = 256$, $2^{2^4} = 65536$, $2^{2^5} = 4294967296$, $2^{2^6} = 18446744073709551616 \ldots$!
Il doit y avoir un rapport entre la logique propositionnelle et les fonctions booléennes :

Logique propositionnelle	Fonctions booléennes
valuation	n-uplet
variable	position
classe d'équivalence de formules	fonction booléenne

Ordre des variables

Pour faire la correspondance entre les variables d'une formule propositionnelle et les positions dans un n-uplet dans $\mathbf{B}^n$, il s'impose de supposer que les variables sont ordonnées. Sans perte de généralité disons que

$$PROP = \{x_1, \ldots, x_n\}.$$

Comme ça la correspondance entre variables et positions est évidente !

Correspondance entre valuations et *n*-uplets

Rappel : une valuation est une fonction $v : PROP \Rightarrow \{0, 1\}$.
Étant donnée une valuation v, elle correspond au n-uplet

$$(v(x_1), \ldots, v(x_n)).$$

Étant donné un n-uplet $(\epsilon_1, \ldots, \epsilon_n)$, il correspond à la valuation

$$\{x_1 \mapsto \epsilon_1, \ldots, x_n \mapsto \epsilon_n\}.$$

On peut dire que $PROP \Rightarrow \{0, 1\}$ et $\mathbf{B}^n$ sont isomorphes.



Correspondance entre valuations et *n*-uplets

Rappel : une valuation est une fonction $v : PROP \Rightarrow \{0,1\}$.
Étant donnée une valuation v, elle correspond au n-uplet

$$(v(x_1), \ldots, v(x_n)).$$

Étant donné un n-uplet $(\epsilon_1, \ldots, \epsilon_n)$, il correspond à la valuation

$$\{x_1 \mapsto \epsilon_1, \ldots, x_n \mapsto \epsilon_n\}.$$

On peut dire que $PROP \Rightarrow \{0,1\}$ et $\mathbf{B}^n$ sont isomorphes.
Exemple : La valuation $\{x_1 \mapsto 0, x_2 \mapsto 1, x_3 \mapsto 0\}$ correspond au triplet $(0,1,0)$ et vice versa.



Correspondance entre formules et fonctions booléennes

Le tableau ci-dessus suggère que chaque classe d'équivalence de formules correspond à une fonction booléenne et vice versa.

Correspondance entre formules et fonctions booléennes

Le tableau ci-dessus suggère que chaque classe d'équivalence de formules correspond à une fonction booléenne et vice versa.
Il faut donc s'attendre qu'à chaque formule correspond une fonction booléenne, mais étant donnée une fonction booléenne f, il y a en général plusieurs formules qui correspondent à f.
Mais on commence par : étant donnée une formule φ, quelle fonction booléenne correspond à φ ?

Une fonction booléenne pour une formule

Rappel : Une interprétation est une fonction
$I : (PROP \Rightarrow \{0,1\}) \Rightarrow FORM \Rightarrow \{0,1\}$, c.-à-d.,
$I : (PROP \Rightarrow \mathbf{B}) \Rightarrow FORM \Rightarrow \mathbf{B}$.



Une fonction booléenne pour une formule

Rappel : Une interprétation est une fonction
$I : (PROP \Rightarrow \{0,1\}) \Rightarrow FORM \Rightarrow \{0,1\}$, c.-à-d.,
$I : (PROP \Rightarrow \mathbf{B}) \Rightarrow FORM \Rightarrow \mathbf{B}$.
Nous définissons f qui correspond de manière évidente à I ; la définition se sert de l'isomorphisme entre $PROP \Rightarrow \mathbf{B}$ et $\mathbf{B}^n$, et f prend les deux arguments dans l'ordre inversé par rapport à I. Alors $f : FORM \Rightarrow \mathbf{B}^n \Rightarrow \mathbf{B}$ est défini par

$$f_\varphi(\epsilon_1, \dots, \epsilon_n) := I_{\{x_1 \mapsto \epsilon_1, \dots, x_n \mapsto \epsilon_n\}}(\varphi)$$

Exemple d'une fonction pour une formule

Soit $n = 3$.

$$
\begin{array}{lcl}
f_{x_1 \wedge \neg x_3}(0,0,0) & = & I_{\{x_1 \mapsto 0, x_2 \mapsto 0, x_3 \mapsto 0\}}(x_1 \wedge \neg x_3) = 0 \\
f_{x_1 \wedge \neg x_3}(0,0,1) & = & I_{\{x_1 \mapsto 0, x_2 \mapsto 0, x_3 \mapsto 1\}}(x_1 \wedge \neg x_3) = 0 \\
f_{x_1 \wedge \neg x_3}(0,1,0) & = & I_{\{x_1 \mapsto 0, x_2 \mapsto 1, x_3 \mapsto 0\}}(x_1 \wedge \neg x_3) = 0 \\
f_{x_1 \wedge \neg x_3}(0,1,1) & = & I_{\{x_1 \mapsto 0, x_2 \mapsto 1, x_3 \mapsto 1\}}(x_1 \wedge \neg x_3) = 0 \\
f_{x_1 \wedge \neg x_3}(1,0,0) & = & I_{\{x_1 \mapsto 1, x_2 \mapsto 0, x_3 \mapsto 0\}}(x_1 \wedge \neg x_3) = 1 \\
f_{x_1 \wedge \neg x_3}(1,0,1) & = & I_{\{x_1 \mapsto 1, x_2 \mapsto 0, x_3 \mapsto 1\}}(x_1 \wedge \neg x_3) = 0 \\
f_{x_1 \wedge \neg x_3}(1,1,0) & = & I_{\{x_1 \mapsto 1, x_2 \mapsto 1, x_3 \mapsto 0\}}(x_1 \wedge \neg x_3) = 1 \\
f_{x_1 \wedge \neg x_3}(1,1,1) & = & I_{\{x_1 \mapsto 1, x_2 \mapsto 1, x_3 \mapsto 1\}}(x_1 \wedge \neg x_3) = 0
\end{array}
$$

Donc $f_{x_1 \wedge \neg x_3}$ est une fonction booléenne de 3 variables qui donne résultat 1 ssi la première position est 1 et la troisième position est 0.



Une formule pour une fonction

Par définition, $f_{x_1 \wedge \neg x_3} = f_{\neg x_3 \wedge x_1}$. En fait, toutes les formules équivalentes à $x_1 \wedge \neg x_3$ correspondent à la même fonction booléenne.
Questions générales :

- Quelle est la formule la plus “naturelle” (la formule canonique) correspondant à une fonction booléenne ?
- Quelle est la formule la plus “simple” correspondant à une fonction booléenne ?

On traite d'abord la première question.

Une notation pour les monômes

Un littéral est une variable propositionnelle ou la négation d'une variable propositionnelle. Un monôme est une conjonction de littéraux.
Exemple : $x_1 \wedge \neg x_3$ est un monôme.
Pour définir la formule canonique correspondant à une fonction booléenne, nous introduisons les notations suivantes : pour une variable x_i et une valeur $\epsilon_i \in \mathbf{B}$,

$$x_i^{\epsilon_i} := \begin{cases} \neg x_i & \text{si } \epsilon_i = 0 \\ x_i & \text{si } \epsilon_i = 1 \end{cases}$$

Une notation pour les monômes

Un littéral est une variable propositionnelle ou la négation d'une variable propositionnelle. Un monôme est une conjonction de littéraux.
Exemple : $x_1 \wedge \neg x_3$ est un monôme.
Pour définir la formule canonique correspondant à une fonction booléenne, nous introduisons les notations suivantes : pour une variable x_i et une valeur $\epsilon_i \in \mathbf{B}$,

$$x_i^{\epsilon_i} := \begin{cases} \neg x_i & \text{si } \epsilon_i = 0 \\ x_i & \text{si } \epsilon_i = 1 \end{cases}$$

Par ailleurs pour $\epsilon = (\epsilon_1, \ldots, \epsilon_n)$ nous définissons

$$x^{\epsilon} := x_1^{\epsilon 1} \wedge \ldots \wedge x_n^{\epsilon n}$$

On appelle x^{ϵ} un monôme canonique, c.-à-d. un monôme qui contient chaque variable soit sans négation soit avec.



Une notation pour les monômes

Un littéral est une variable propositionnelle ou la négation d'une variable propositionnelle. Un monôme est une conjonction de littéraux.
Exemple : $x_1 \wedge \neg x_3$ est un monôme.
Pour définir la formule canonique correspondant à une fonction booléenne, nous introduisons les notations suivantes : pour une variable x_i et une valeur $\epsilon_i \in \mathbf{B}$,

$$x_i^{\epsilon_i} := \begin{cases} \neg x_i & \text{si } \epsilon_i = 0 \\ x_i & \text{si } \epsilon_i = 1 \end{cases}$$

Par ailleurs pour $\epsilon = (\epsilon_1, \dots, \epsilon_n)$ nous définissons

$$x^{\epsilon} := x_1^{\epsilon_1} \wedge \dots \wedge x_n^{\epsilon_n}$$

On appelle x^{ϵ} un monôme canonique, c.-à-d. un monôme qui contient chaque variable soit sans négation soit avec.
Exemple : $x^{(1,1,0)} = x_1 \wedge x_2 \wedge \neg x_3$.

À quoi sert x^ϵ ?

Soient $\epsilon = (\epsilon_1, \ldots, \epsilon_n) \in \mathbf{B}^n$ et $\delta = (\delta_1, \ldots, \delta_n) \in \mathbf{B}^n$. Par définition

$$f_{x^\epsilon}(\delta_1, \ldots, \delta_n) = I_{\{x_1 \mapsto \delta_1, \ldots, x_n \mapsto \delta_n\}}(x_1^{\epsilon_1} \wedge \ldots \wedge x_n^{\epsilon_n})$$

Mais pour chaque $i \in \{1, \ldots, n\}$, on a $v(x_i^{\epsilon_i}) = 1$ ssi soit $v(x_i) = 1$ et $\epsilon_i = 1$ (x_i apparaît sans négation), soit $v(x_i) = 0$ et $\epsilon_i = 0$ (x_i apparaît avec négation), en bref : $v(x_i^{\epsilon_i}) = 1$ ssi $v(x_i) = \epsilon_i$.

À quoi sert x^ϵ ?

Soient $\epsilon = (\epsilon_1, \ldots, \epsilon_n) \in \mathbf{B}^n$ et $\delta = (\delta_1, \ldots, \delta_n) \in \mathbf{B}^n$. Par définition

$$f_{x^\epsilon}(\delta_1, \ldots, \delta_n) = I_{\{x_1 \mapsto \delta_1, \ldots, x_n \mapsto \delta_n\}}(x_1^{\epsilon_1} \wedge \ldots \wedge x_n^{\epsilon_n})$$

Mais pour chaque $i \in \{1, \ldots, n\}$, on a $v(x_i^{\epsilon_i}) = 1$ ssi soit $v(x_i) = 1$ et $\epsilon_i = 1$ (x_i apparaît sans négation), soit $v(x_i) = 0$ et $\epsilon_i = 0$ (x_i apparaît avec négation), en bref : $v(x_i^{\epsilon_i}) = 1$ ssi $v(x_i) = \epsilon_i$.
Comme il s'agit d'une conjonction, il suit que
$I_{\{x_1 \mapsto \delta_1, \ldots, x_n \mapsto \delta_n\}}(x_1^{\epsilon_1} \wedge \ldots \wedge x_n^{\epsilon_n}) = 1$ ssi $\epsilon = \delta$, c.-à-d. la valuation $\{x_1 \mapsto \delta_1, \ldots, x_n \mapsto \delta_n\}$ doit rendre vraies exactement les variables qui apparaissent dans $x_1^{\epsilon_1} \wedge \ldots \wedge x_n^{\epsilon_n}$ sans négation.
x^ϵ est donc le représentant évident pour la fonction booléenne qui vaut 1 exactement pour le n-uplet ϵ.
Exemple : $x^{(1,1,0)} = x_1 \wedge x_2 \wedge \neg x_3$ représente la fonction qui vaut 1 exactement pour $(1, 1, 0)$ et 0 ailleurs.

La notation s'alourdit . . .

On a utilisé la notation $\epsilon = (\epsilon_1, \ldots, \epsilon_n)$ pour noter un *n*-uplet. Pour noter un ensemble de plusieurs, disons *m*, *n*-uplets, nous utilisons la notation $\epsilon^1 = (\epsilon_1^1, \ldots, \epsilon_n^1), \ldots, \epsilon^m = (\epsilon_1^m, \ldots, \epsilon_n^m)$.
Exemple : pour l'ensemble {(1,0,1),(1,1,1)} on a $n = 3$ et $m = 2$.



La formule canonique pour f

Soit f la fonction booléenne qui vaut 1 exactement pour les n-uplets $\epsilon^1 = (\epsilon^1_1, \ldots, \epsilon^1_n), \ldots, \epsilon^m = (\epsilon^m_1, \ldots, \epsilon^m_n)$.
Alors $x^{\epsilon^1} \vee \ldots \vee x^{\epsilon^m}$ correspond à f, c.-à-d.

$$f_{x^{\epsilon^1} \vee \ldots \vee x^{\epsilon^m}} = f$$

La formule canonique pour f

Soit f la fonction booléenne qui vaut 1 exactement pour les n-uplets $\epsilon^1 = (\epsilon_1^1, \ldots, \epsilon_n^1), \ldots, \epsilon^m = (\epsilon_1^m, \ldots, \epsilon_n^m)$.
Alors $x^{\epsilon^1} \vee \ldots \vee x^{\epsilon^m}$ correspond à f, c.-à-d.

$$f_{x^{\epsilon^1} \vee \ldots \vee x^{\epsilon^m}} = f$$

Esquisse de preuve : Par définition, pour un n-uplet $\delta = (\delta_1, \ldots, \delta_n) \in \mathbf{B}^n$

$$f_{x^{\epsilon^1} \vee \ldots \vee x^{\epsilon^m}}(\delta_1, \ldots, \delta_n) = I_{\{x_1 \mapsto \delta_1, \ldots, x_n \mapsto \delta_n\}}(x^{\epsilon^1} \vee \ldots \vee x^{\epsilon^m})$$

Cette expression vaut 1 ssi

$$I_{\{x_1 \mapsto \delta_1, \ldots, x_n \mapsto \delta_n\}}(x^{\epsilon^j}) = 1$$

pour au moins un $j \in \{1, \ldots, m\}$. Et $I_{\{x_1 \mapsto \delta_1, \ldots, x_n \mapsto \delta_n\}}(x^{\epsilon^j}) = 1$ ssi $(\delta_1, \ldots, \delta_n) = \epsilon^j$.

Exemple de la formule canonique pour f

Soit f la fonction booléenne qui vaut 1 exactement pour les triplets $(1,0,0)$, $(1,1,0)$.
Alors $x^{(1,0,0)} \vee x^{(1,1,0)} = (x_1^1 \wedge x_2^0 \wedge x_3^0) \vee (x_1^1 \wedge x_2^1 \wedge x_3^0) = (x_1 \wedge \neg x_2 \wedge \neg x_3) \vee (x_1 \wedge x_2 \wedge \neg x_3)$ correspond à f.
En fait,

$$f_{(x_1 \wedge \neg x_2 \wedge \neg x_3) \vee (x_1 \wedge x_2 \wedge \neg x_3)}(1,0,0) = I_{\{x_1 \mapsto 1, x_2 \mapsto 0, x_3 \mapsto 0\}}((x_1 \wedge \neg x_2 \wedge \neg x_3) \vee (x_1 \wedge x_2 \wedge \neg x_3)) = 1$$

$$f_{(x_1 \wedge \neg x_2 \wedge \neg x_3) \vee (x_1 \wedge x_2 \wedge \neg x_3)}(1,1,0) = I_{\{x_1 \mapsto 1, x_2 \mapsto 1, x_3 \mapsto 0\}}((x_1 \wedge \neg x_2 \wedge \neg x_3) \vee (x_1 \wedge x_2 \wedge \neg x_3)) = 1$$

et $f_{(x_1 \wedge \neg x_2 \wedge \neg x_3) \vee (x_1 \wedge x_2 \wedge \neg x_3)}(\delta_1, \delta_2, \delta_3) = 0$ pour tout $(\delta_1, \delta_2, \delta_3) \notin \{(1,0,0), (1,1,0)\}$.



Formule canonique : résumé

- Soit f une fonction booléenne qui vaut 1 pour exactement m n-uplets (f a m “n-uplets vrais”). La formule canonique qui représente f est une disjonction de m monômes canoniques.
- Chaque monôme canonique est une conjonction de n littéraux basés sur $x_1, \ldots, x_n$. Il correspond à exactement un n-uplet vrai de f.
- Chaque variable du monôme apparaît sans négation pour représenter un 1 dans le n-uplet, et apparaît avec négation pour représenter un 0 dans le n-uplet.

Une notation bien lourde pour exprimer une idée simple !

Formule canonique : résumé

- Soit f une fonction booléenne qui vaut 1 pour exactement m n-uplets (f a m “n-uplets vrais”). La formule canonique qui représente f est une disjonction de m monômes canoniques.
- Chaque monôme canonique est une conjonction de n littéraux basés sur $x_1, \ldots, x_n$. Il correspond à exactement un n-uplet vrai de f.
- Chaque variable du monôme apparaît sans négation pour représenter un 1 dans le n-uplet, et apparaît avec négation pour représenter un 0 dans le n-uplet.

Une notation bien lourde pour exprimer une idée simple !

Exercice : donnez la formule canonique pour la fonction booléenne qui vaut 1 exactement pour les quadruplets $(1, 0, 0, 1)$, $(0, 1, 1, 0)$, $(1, 0, 1, 0)$.

Formule canonique : résumé

- Soit f une fonction booléenne qui vaut 1 pour exactement m n-uplets (f a m “n-uplets vrais”). La formule canonique qui représente f est une disjonction de m monômes canoniques.
- Chaque monôme canonique est une conjonction de n littéraux basés sur $x_1, \ldots, x_n$. Il correspond à exactement un n-uplet vrai de f.
- Chaque variable du monôme apparaît sans négation pour représenter un 1 dans le n-uplet, et apparaît avec négation pour représenter un 0 dans le n-uplet.

Une notation bien lourde pour exprimer une idée simple !

Exercice : donnez la formule canonique pour la fonction booléenne qui vaut 1 exactement pour les quadruplets $(1, 0, 0, 1)$, $(0, 1, 1, 0)$, $(1, 0, 1, 0)$.

Maintenant la deuxième question . . .



Une formule simple en utilisant quels connecteurs ?

Question : quelle est la formule la plus “simple” correspondant à une fonction booléenne ?

Pour préciser :

- Que veut dire “simple” ?

Une formule simple en utilisant quels connecteurs ?

Question : quelle est la formule la plus “simple” correspondant à une fonction booléenne ?
Pour préciser :

- Que veut dire “simple” ? Pas très important, supposons la taille (nombre de symboles) de la formule.
- Les connecteurs ($\neg$, $\wedge$, $\vee$, $\rightarrow$) sont les “briques de base” pour représenter une fonction. Mais peut-être pourrait-on utiliser d'autres connecteurs comme $\leftrightarrow$ ou $\oplus$, ou inventer de nouveaux connecteurs ?

Une formule simple en utilisant quels connecteurs ?

Question : quelle est la formule la plus “simple” correspondant à une fonction booléenne ?
Pour préciser :

- Que veut dire “simple” ? Pas très important, supposons la taille (nombre de symboles) de la formule.
- Les connecteurs ($\neg$, $\wedge$, $\vee$, $\rightarrow$) sont les “briques de base” pour représenter une fonction. Mais peut-être pourrait-on utiliser d’autres connecteurs comme $\leftrightarrow$ ou $\oplus$, ou inventer de nouveaux connecteurs ?
  A ce niveau, le problème de trouver une représentation la plus simple possible est un problème extrêmement difficile !

Une formule simple en utilisant quels connecteurs ?

Question : quelle est la formule la plus “simple” correspondant à une fonction booléenne ?
Pour préciser :

- Que veut dire “simple” ? Pas très important, supposons la taille (nombre de symboles) de la formule.
- Les connecteurs ($\neg$, $\wedge$, $\vee$, $\rightarrow$) sont les “briques de base” pour représenter une fonction. Mais peut-être pourrait-on utiliser d’autres connecteurs comme $\leftrightarrow$ ou $\oplus$, ou inventer de nouveaux connecteurs ?
  A ce niveau, le problème de trouver une représentation la plus simple possible est un problème extrêmement difficile !
- Même si on se limite à $\neg$, $\wedge$, $\vee$, $\rightarrow$, le problème reste très difficile.

On n'utilise que des disjonctions de monômes

- Nous allons nous limiter à des disjonctions de monômes, par exemple $(x_1 \wedge x_2) \vee (x_1 \wedge x_3)$. Cette formule n'est pas la plus simple dans l'absolu, car elle est équivalente à $x_1 \wedge (x_2 \vee x_3)$.
- Nous ne regardons que les monômes non-contradictoires, c.-à-d., des monômes qui ne contiennent pas x_i et $\neg x_i$.

Simplifier deux monômes

Exemple : les deux monômes de $(x_1 \wedge \neg x_2 \wedge \neg x_3) \vee (x_1 \wedge x_2 \wedge \neg x_3)$ sont identiques au signe de x_2 près. La formule $(x_1 \wedge \neg x_2 \wedge \neg x_3) \vee (x_1 \wedge x_2 \wedge \neg x_3)$ est équivalente à $x_1 \wedge \neg x_3$.
En général,

$$(C \wedge x_i) \vee (C \wedge \neg x_i) \equiv C.$$

Cette équivalence peut être utilisée pour simplifier les formules canoniques.

Exemple de simplification

$$(x_1 \wedge x_2 \wedge x_3 \wedge x_4) \vee (x_1 \wedge \neg x_2 \wedge x_3 \wedge x_4) \vee$$
$$(x_1 \wedge x_2 \wedge \neg x_3 \wedge x_4) \vee (x_1 \wedge \neg x_2 \wedge \neg x_3 \wedge x_4) \vee$$
$$(\neg x_1 \wedge x_2 \wedge x_3 \wedge \neg x_4) \vee (\neg x_1 \wedge \neg x_2 \wedge x_3 \wedge \neg x_4) \vee$$
$$(\neg x_1 \wedge x_2 \wedge \neg x_3 \wedge \neg x_4) \vee (\neg x_1 \wedge \neg x_2 \wedge \neg x_3 \wedge \neg x_4) \equiv$$

$$(x_1 \wedge x_3 \wedge x_4) \vee (x_1 \wedge \neg x_3 \wedge x_4) \vee$$
$$(\neg x_1 \wedge x_3 \wedge \neg x_4) \vee (\neg x_1 \wedge \neg x_3 \wedge \neg x_4) \equiv$$

$$(x_1 \wedge x_4) \vee (\neg x_1 \wedge \neg x_4)$$

Autre exemple de simplification

$$(x_1 \wedge x_2) \vee (\neg x_1 \wedge x_2) \vee (x_1 \wedge \neg x_2) \equiv x_2 \vee (x_1 \wedge \neg x_2)$$

mais aussi

$$(x_1 \wedge x_2) \vee (\neg x_1 \wedge x_2) \vee (x_1 \wedge \neg x_2) \equiv x_1 \vee (\neg x_1 \wedge x_2)$$

Autre exemple de simplification

$$(x_1 \wedge x_2) \vee (\neg x_1 \wedge x_2) \vee (x_1 \wedge \neg x_2) \equiv$$
$$x_2 \vee (x_1 \wedge \neg x_2)$$

mais aussi

$$(x_1 \wedge x_2) \vee (\neg x_1 \wedge x_2) \vee (x_1 \wedge \neg x_2) \equiv$$
$$x_1 \vee (\neg x_1 \wedge x_2)$$

mais aussi (et c'est moins évident)

$$(x_1 \wedge x_2) \vee (\neg x_1 \wedge x_2) \vee (x_1 \wedge \neg x_2) \equiv$$
$$(x_1 \wedge x_2) \vee x_2 \vee (x_1 \wedge \neg x_2) \equiv$$
$$x_1 \vee x_2$$

Comment ça s'explique ?



Monômes maximaux

Soit $C_1 \vee \ldots \vee C_m$ une disjonction de monômes. On dit que C_j est maximal dans $C_1 \vee \ldots \vee C_m$ s'il n'y a pas de $k \neq j$ tel que $\models C_j \rightarrow C_k$ (en considérant C_k, C_j comme ensembles de littéraux : $C_k \subseteq C_j$).
Exemple : dans $(x_1 \wedge x_2) \vee x_2 \vee (x_1 \wedge \neg x_2)$, le monôme x_2 est maximal mais $x_1 \wedge x_2$ n'est pas maximal car $\models x_1 \wedge x_2 \rightarrow x_2$ ($\{x_2\} \subseteq \{x_1, x_2\}$).
À retenir : les monômes maximaux sont des monômes courts.

Monômes maximaux

Soit $C_1 \vee \ldots \vee C_m$ une disjonction de monômes. On dit que C_j est maximal dans $C_1 \vee \ldots \vee C_m$ s'il n'y a pas de $k \neq j$ tel que $\models C_j \rightarrow C_k$ (en considérant C_k, C_j comme ensembles de littéraux : $C_k \subseteq C_j$).
Exemple : dans $(x_1 \wedge x_2) \vee x_2 \vee (x_1 \wedge \neg x_2)$, le monôme x_2 est maximal mais $x_1 \wedge x_2$ n'est pas maximal car $\models x_1 \wedge x_2 \rightarrow x_2$ ($\{x_2\} \subseteq \{x_1, x_2\}$).
À retenir : les monômes maximaux sont des monômes courts.

Lemme : Soit C_j un monôme non-maximal dans $C_1 \vee \ldots \vee C_m$. Alors

$$C_1 \vee \ldots \vee C_m \equiv C_1 \vee \ldots \vee C_{j-1} \vee C_{j+1} \vee \ldots \vee C_m$$

Donc si on veut une formule simple, clairement on ne retiendra jamais des monômes non-maximaux !
Mais est-ce que cela veut dire qu'il faut éliminer les monômes non-maximaux dès qu'on les rencontre ? ...

Exemple revisité

$$(x_1 \wedge x_2) \vee (\neg x_1 \wedge x_2) \vee (x_1 \wedge \neg x_2)$$

On a utilisé l'équivalence $(x_1 \wedge x_2) \vee (\neg x_1 \wedge x_2) \equiv x_2$ mais mystérieusement on a gardé le monôme $x_1 \wedge x_2$ pour obtenir

$$(x_1 \wedge x_2) \vee x_2 \vee (x_1 \wedge \neg x_2).$$

Ensuite on a utilisé l'équivalence $(x_1 \wedge x_2) \vee (x_1 \wedge \neg x_2) \equiv x_1$ pour obtenir

$$x_1 \vee x_2.$$



Exemple revisité

$$(x_1 \wedge x_2) \vee (\neg x_1 \wedge x_2) \vee (x_1 \wedge \neg x_2)$$

On a utilisé l'équivalence $(x_1 \wedge x_2) \vee (\neg x_1 \wedge x_2) \equiv x_2$ mais mystérieusement on a gardé le monôme $x_1 \wedge x_2$ pour obtenir

$$(x_1 \wedge x_2) \vee x_2 \vee (x_1 \wedge \neg x_2).$$

Ensuite on a utilisé l'équivalence $(x_1 \wedge x_2) \vee (x_1 \wedge \neg x_2) \equiv x_1$ pour obtenir

$$x_1 \vee x_2.$$

Comment faire en général ? Il faut encore un concept ...



Monômes centraux

Soit $C_1 \vee \ldots \vee C_m$ une disjonction de monômes tous maximaux dans $C_1 \vee \ldots \vee C_m$. On dit que C_j est central dans $C_1 \vee \ldots \vee C_m$ si

$$\not\models C_j \rightarrow C_1 \vee \ldots \vee C_{j-1} \vee C_{j+1} \vee \ldots \vee C_m$$

Monômes centraux

Soit $C_1 \vee \ldots \vee C_m$ une disjonction de monômes tous maximaux dans $C_1 \vee \ldots \vee C_m$. On dit que C_j est central dans $C_1 \vee \ldots \vee C_m$ si

$$\not\models C_j \rightarrow C_1 \vee \ldots \vee C_{j-1} \vee C_{j+1} \vee \ldots \vee C_m$$

Exemple : dans $(x_2 \wedge x_3) \vee (x_1 \wedge \neg x_3) \vee (x_1 \wedge x_2)$, les monômes $x_2 \wedge x_3$ et $x_1 \wedge \neg x_3$ sont centraux mais $x_1 \wedge x_2$ n'est pas central car $\models x_1 \wedge x_2 \rightarrow (x_2 \wedge x_3) \vee (x_1 \wedge \neg x_3)$.
Le vrai triplet $(0, 1, 1)$ n'est “couvert” que par $x_2 \wedge x_3$.
Le vrai triplet $(1, 0, 0)$ n'est “couvert” que par $x_1 \wedge \neg x_3$.

Monômes centraux

Soit $C_1 \vee \ldots \vee C_m$ une disjonction de monômes tous maximaux dans $C_1 \vee \ldots \vee C_m$. On dit que C_j est central dans $C_1 \vee \ldots \vee C_m$ si

$$\not\models C_j \to C_1 \vee \ldots \vee C_{j-1} \vee C_{j+1} \vee \ldots \vee C_m$$

Exemple : dans $(x_2 \wedge x_3) \vee (x_1 \wedge \neg x_3) \vee (x_1 \wedge x_2)$, les monômes $x_2 \wedge x_3$ et $x_1 \wedge \neg x_3$ sont centraux mais $x_1 \wedge x_2$ n'est pas central car $\models x_1 \wedge x_2 \to (x_2 \wedge x_3) \vee (x_1 \wedge \neg x_3)$.
Le vrai triplet $(0, 1, 1)$ n'est "couvert" que par $x_2 \wedge x_3$.
Le vrai triplet $(1, 0, 0)$ n'est "couvert" que par $x_1 \wedge \neg x_3$.

Lemme : Soit C_j un monôme central dans $C_1 \vee \ldots \vee C_m$. Alors

$$C_1 \vee \ldots \vee C_m \not\equiv C_1 \vee \ldots \vee C_{j-1} \vee C_{j+1} \vee \ldots \vee C_m$$

Donc le monômes centraux sont indispensables !



Monômes maximaux pour une fonction

Nous avons défini un monôme maximal dans $C_1 \vee \ldots \vee C_m$, mais intuitivement, $C_1 \vee \ldots \vee C_m$ correspond à une fonction booléenne, et c'est plutôt la maximalité par rapport à cette fonction qui nous intéresse.

Monômes maximaux pour une fonction

Nous avons défini un monôme maximal dans $C_1 \vee \ldots \vee C_m$, mais intuitivement, $C_1 \vee \ldots \vee C_m$ correspond à une fonction booléenne, et c'est plutôt la maximalité par rapport à cette fonction qui nous intéresse.
Formellement, soit f une fonction booléenne. On dit que C est maximal pour f si

- pour tout $\epsilon = (\epsilon_1, \ldots, \epsilon_n)$, $f_C(\epsilon) = 1$ implique $f(\epsilon) = 1$ ("C ne couvre que des points vrais de f") ;
- pour tout $C' \subset C$, il existe $\epsilon = (\epsilon_1, \ldots, \epsilon_n)$ tel que $f_{C'}(\epsilon) = 1$ et $f(\epsilon) = 0$ ("toute extension de C, en supprimant un littéral, couvrirait trop de points").

Monômes maximaux pour une fonction

Nous avons défini un monôme maximal dans $C_1 \vee \ldots \vee C_m$, mais intuitivement, $C_1 \vee \ldots \vee C_m$ correspond à une fonction booléenne, et c'est plutôt la maximalité par rapport à cette fonction qui nous intéresse.

Formellement, soit f une fonction booléenne. On dit que C est maximal pour f si

- pour tout $\epsilon = (\epsilon_1, \ldots, \epsilon_n)$, $f_C(\epsilon) = 1$ implique $f(\epsilon) = 1$ ("C ne couvre que des points vrais de f") ;
- pour tout $C' \subset C$, il existe $\epsilon = (\epsilon_1, \ldots, \epsilon_n)$ tel que $f_{C'}(\epsilon) = 1$ et $f(\epsilon) = 0$ ("toute extension de C, en supprimant un littéral, couvrirait trop de points").

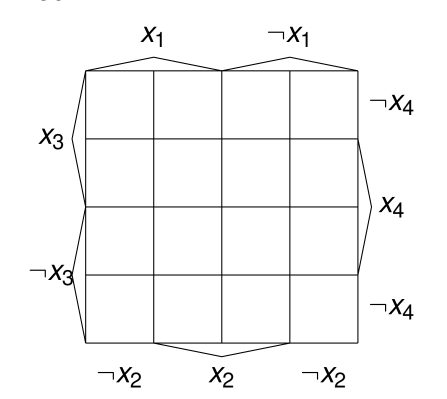
Cette définition est parfaitement cohérente avec la précédente.



Karnaugh

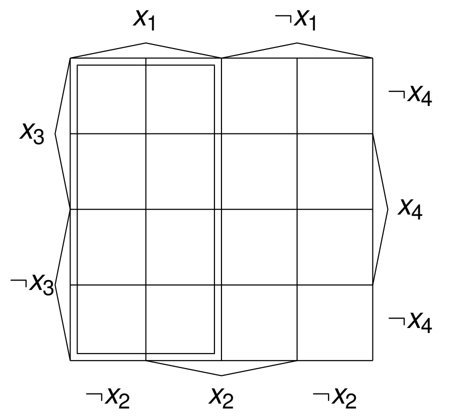
Pour mieux trouver les monômes maximaux, il y a une méthode graphique inventée par Maurice Karnaugh. Elle marche bien pour $n \leq 4$. L'idée est d'arranger les monômes canoniques tel que les monômes ne différant que dans une position soient voisins.

Pour $n = 4$:



C'est un carré mais il faut l'imaginer comme un tore.

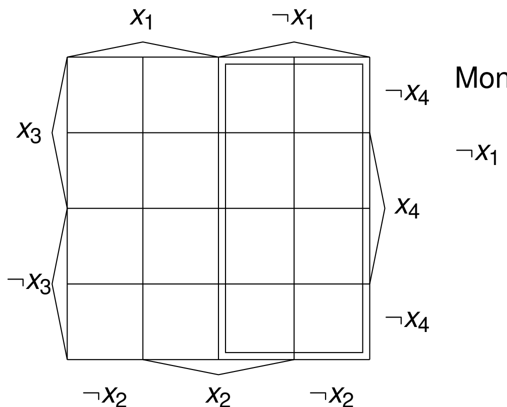
Karnaugh : tous les monômes



Monômes avec 1 variable :

x_1

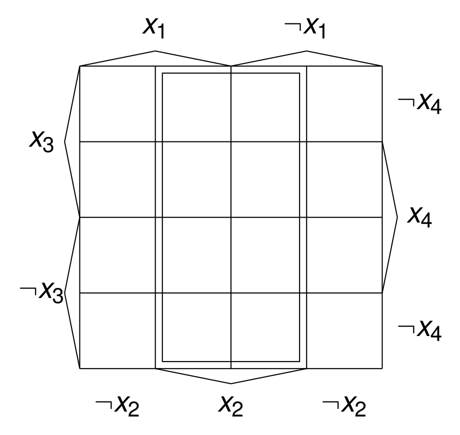
Karnaugh : tous les monômes



Monômes avec 1 variable :

$\neg x_1$

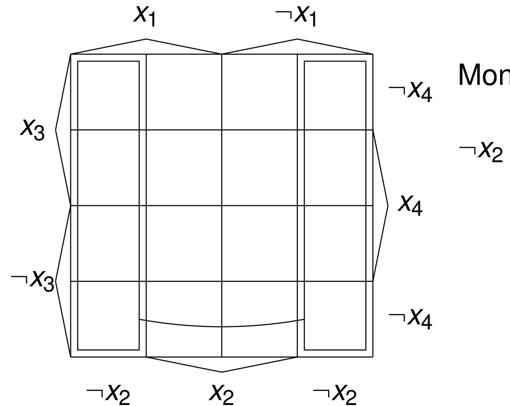
Karnaugh : tous les monômes



Monômes avec 1 variable :

x_2

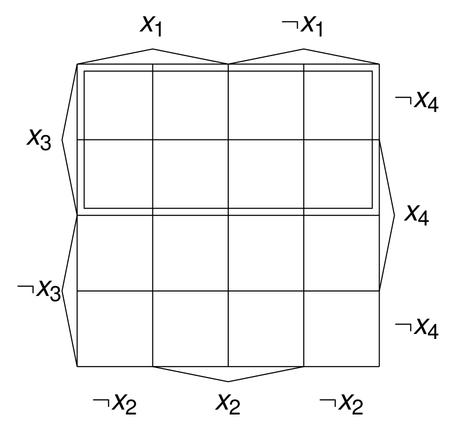
Karnaugh : tous les monômes



Monômes avec 1 variable :

$\neg x_2$

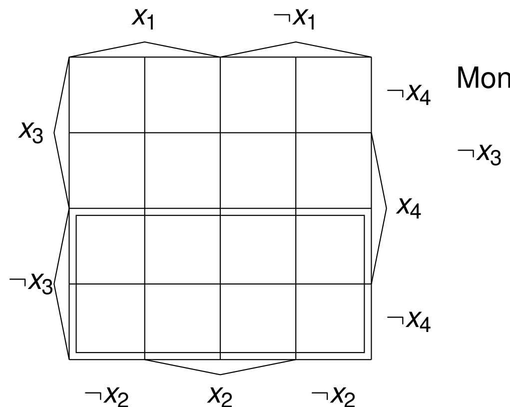
Karnaugh : tous les monômes



Monômes avec 1 variable :

x_3

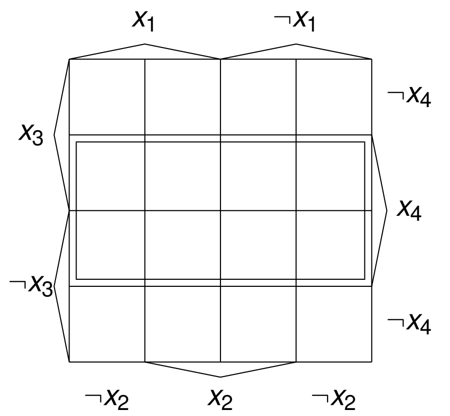
Karnaugh : tous les monômes



Monômes avec 1 variable :

$\neg x_3$

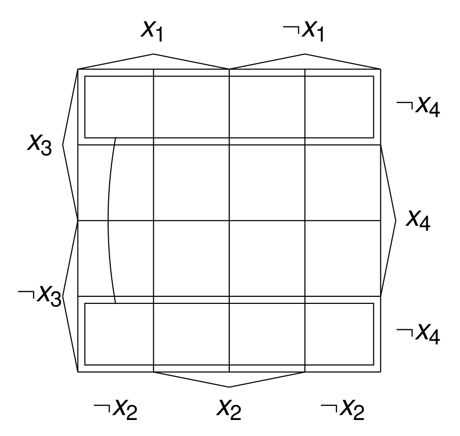
Karnaugh : tous les monômes



Monômes avec 1 variable :

x_4

Karnaugh : tous les monômes

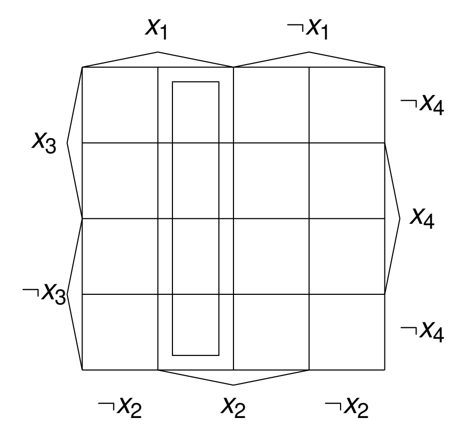


Monômes avec 1 variable :

$\neg x_4$

$\binom{4}{1} \cdot 2^1 = 8$ en total

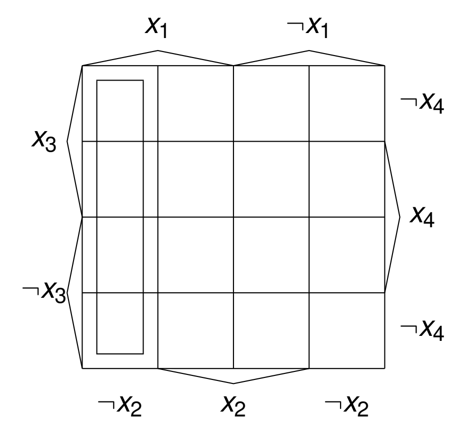
Karnaugh : tous les monômes



Monômes avec 2 variables :

$x_1 \wedge x_2$

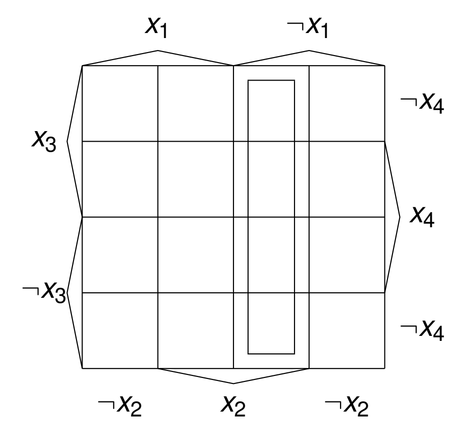
Karnaugh : tous les monômes



Monômes avec 2 variables :

$x_1 \wedge \neg x_2$

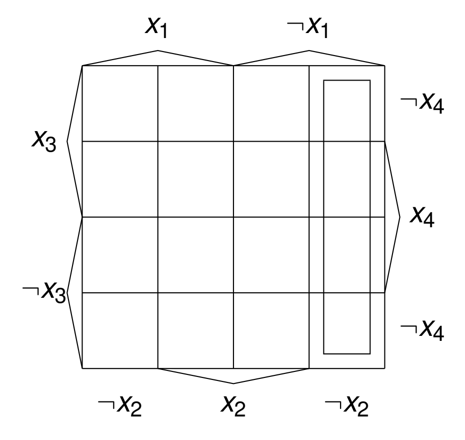
Karnaugh : tous les monômes



Monômes avec 2 variables :

$\neg x_1 \wedge x_2$

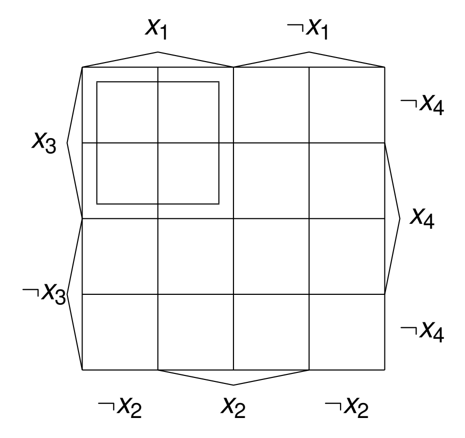
Karnaugh : tous les monômes



Monômes avec 2 variables :

$\neg x_1 \wedge \neg x_2$

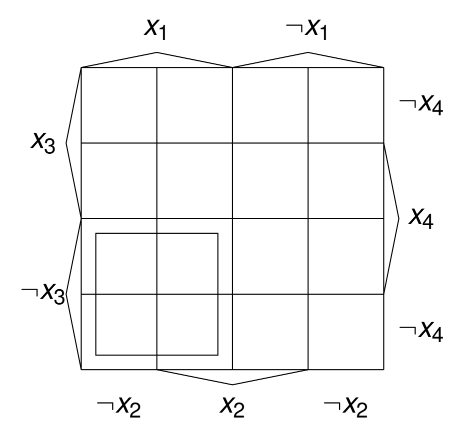
Karnaugh : tous les monômes



Monômes avec 2 variables :

$x_1 \wedge x_3$

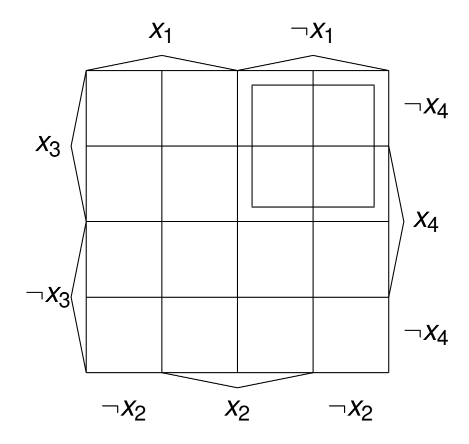
Karnaugh : tous les monômes



Monômes avec 2 variables :

$x_1 \wedge \neg x_3$

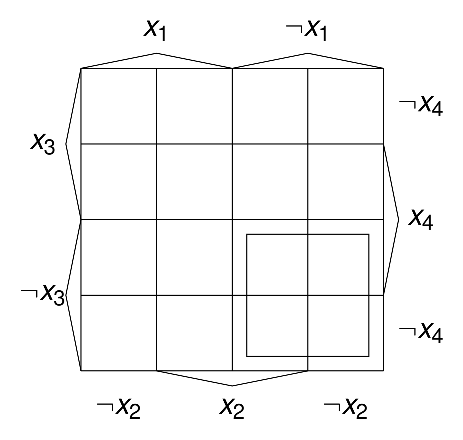
Karnaugh : tous les monômes



Monômes avec 2 variables :

$\neg x_1 \wedge x_3$

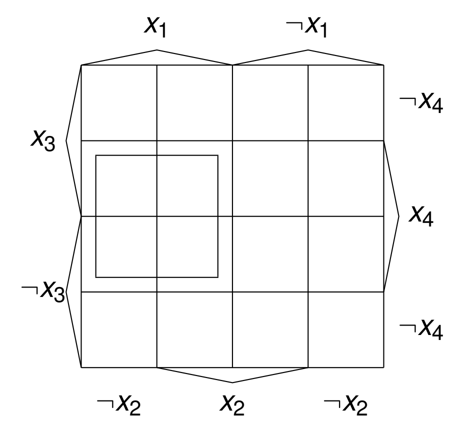
Karnaugh : tous les monômes



Monômes avec 2 variables :

$\neg x_1 \wedge \neg x_3$

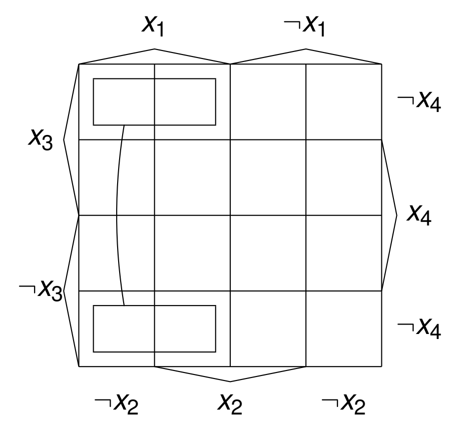
Karnaugh : tous les monômes



Monômes avec 2 variables :

$x_1 \wedge x_4$

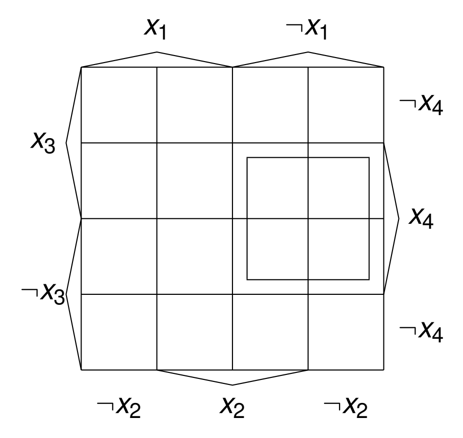
Karnaugh : tous les monômes



Monômes avec 2 variables :

$x_1 \wedge \neg x_4$

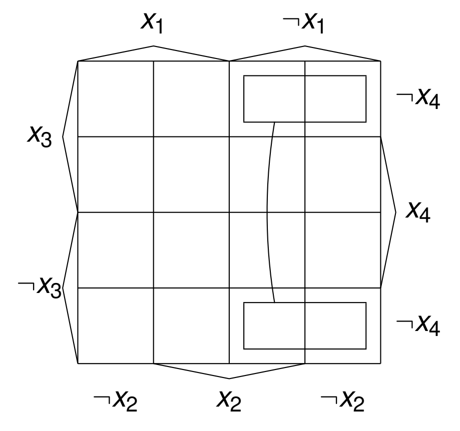
Karnaugh : tous les monômes



Monômes avec 2 variables :

$\neg x_1 \wedge x_4$

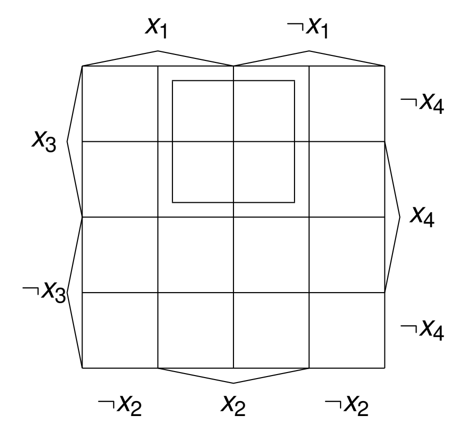
Karnaugh : tous les monômes



Monômes avec 2 variables :

$\neg x_1 \wedge \neg x_4$

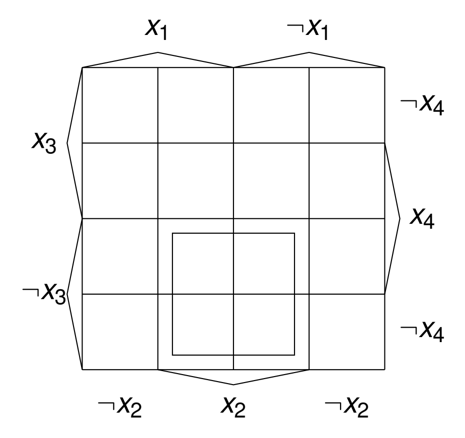
Karnaugh : tous les monômes



Monômes avec 2 variables :

$x_2 \wedge x_3$

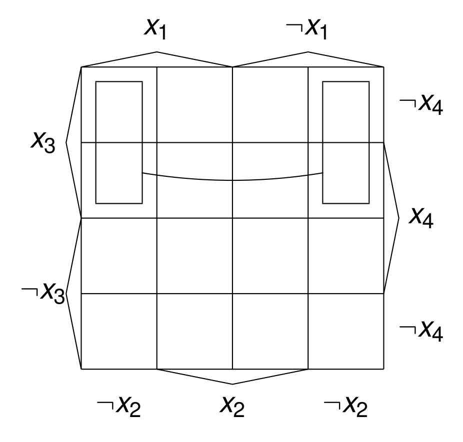
Karnaugh : tous les monômes



Monômes avec 2 variables :

$x_2 \wedge \neg x_3$

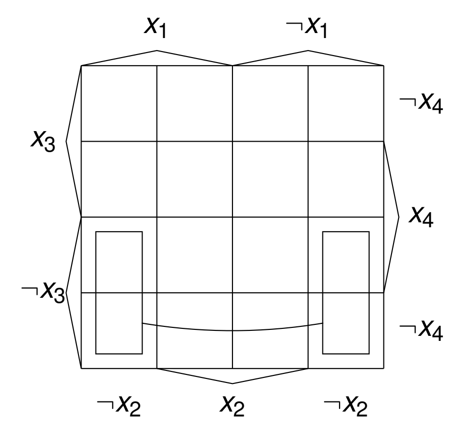
Karnaugh : tous les monômes



Monômes avec 2 variables :

$\neg x_2 \wedge x_3$

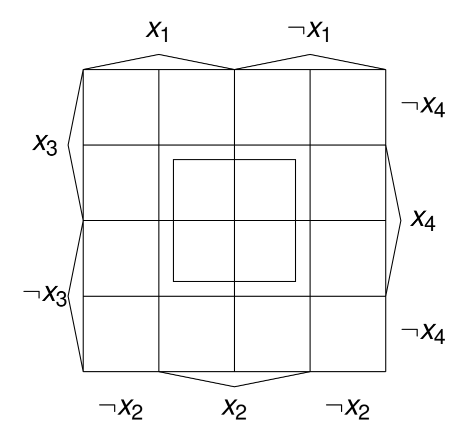
Karnaugh : tous les monômes



Monômes avec 2 variables :

$\neg x_2 \wedge \neg x_3$

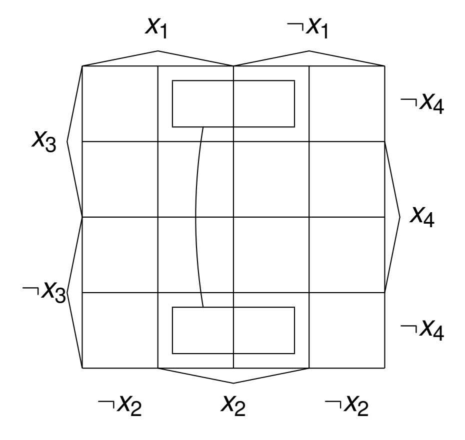
Karnaugh : tous les monômes



Monômes avec 2 variables :

$x_2 \wedge x_4$

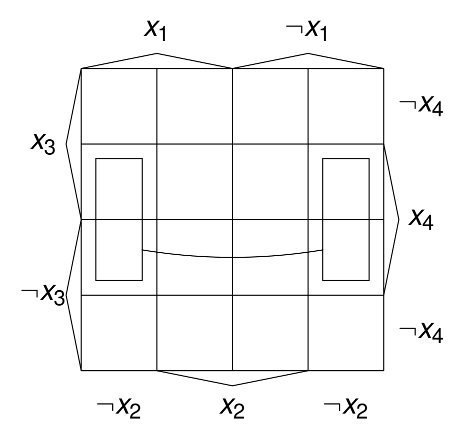
Karnaugh : tous les monômes



Monômes avec 2 variables :

$x_2 \wedge \neg x_4$

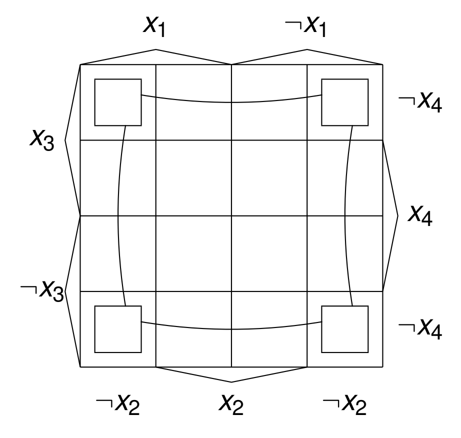
Karnaugh : tous les monômes



Monômes avec 2 variables :

$\neg x_2 \land x_4$

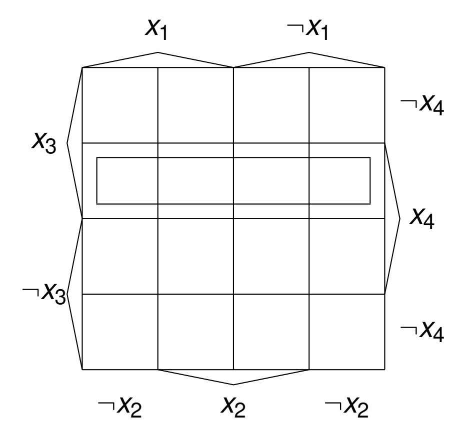
Karnaugh : tous les monômes



Monômes avec 2 variables :

$\neg x_2 \land \neg x_4$

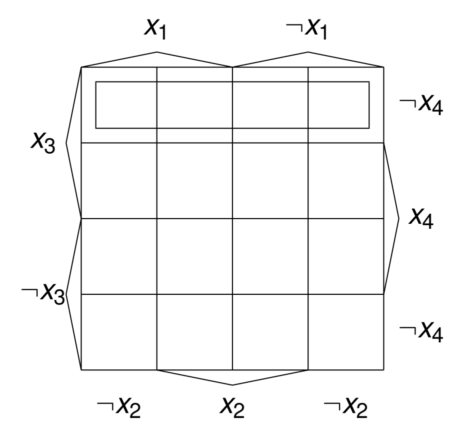
Karnaugh : tous les monômes



Monômes avec 2 variables :

$x_3 \wedge x_4$

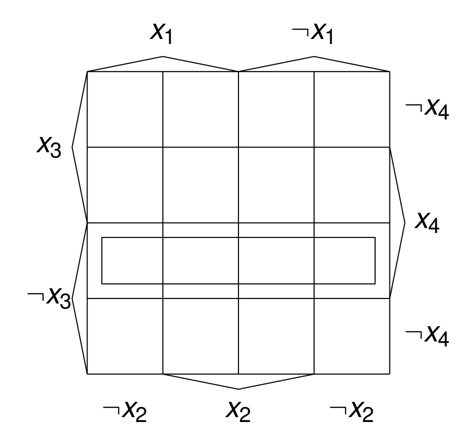
Karnaugh : tous les monômes



Monômes avec 2 variables :

$x_3 \wedge \neg x_4$

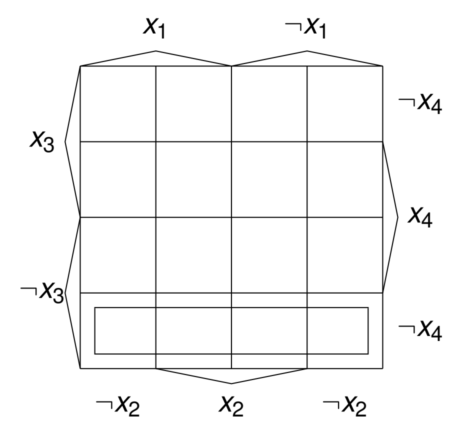
Karnaugh : tous les monômes



Monômes avec 2 variables :

$\neg x_3 \wedge x_4$

Karnaugh : tous les monômes

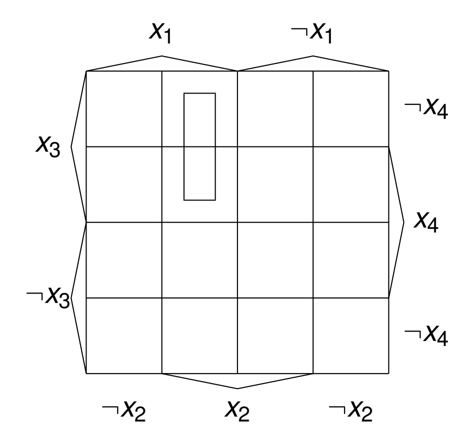


Monômes avec 2 variables :

$\neg x_3 \wedge \neg x_4$

$\binom{4}{2} \cdot 2^2 = 24$ en total

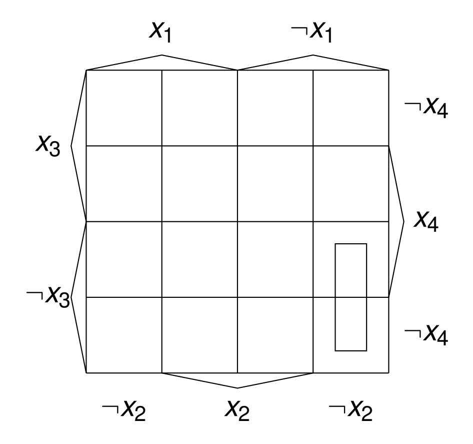
Karnaugh : tous les monômes



Monômes avec 3 variables (exemples) :

$x_1 \wedge x_2 \wedge x_3$

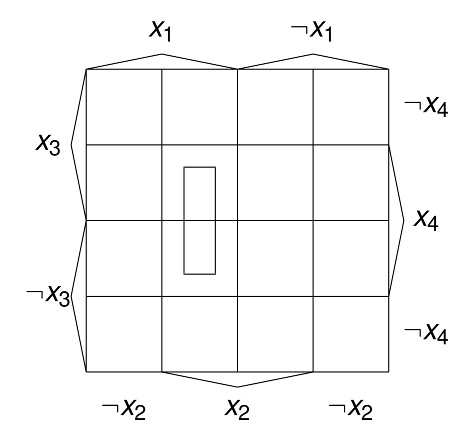
Karnaugh : tous les monômes



Monômes avec 3 variables (exemples) :

$\neg x_1 \wedge \neg x_2 \wedge \neg x_3$

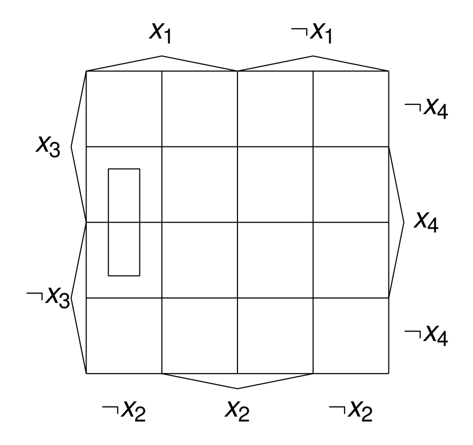
Karnaugh : tous les monômes



Monômes avec 3 variables (exemples) :

$x_1 \wedge x_2 \wedge x_4$

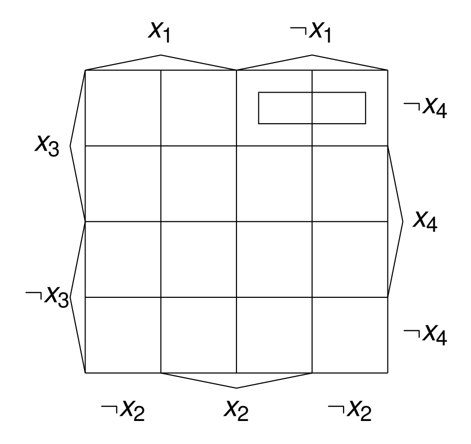
Karnaugh : tous les monômes



Monômes avec 3 variables (exemples) :

$x_1 \wedge \neg x_2 \wedge x_4$

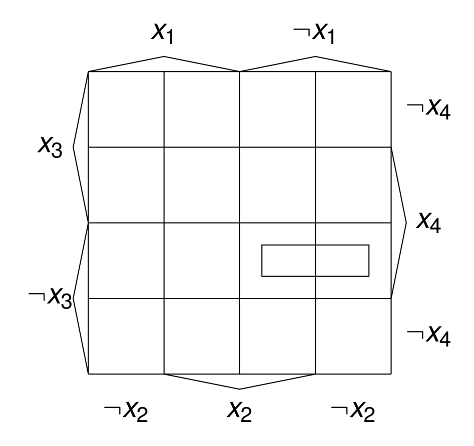
Karnaugh : tous les monômes



Monômes avec 3 variables (exemples) :

$\neg x_1 \wedge x_3 \wedge \neg x_4$

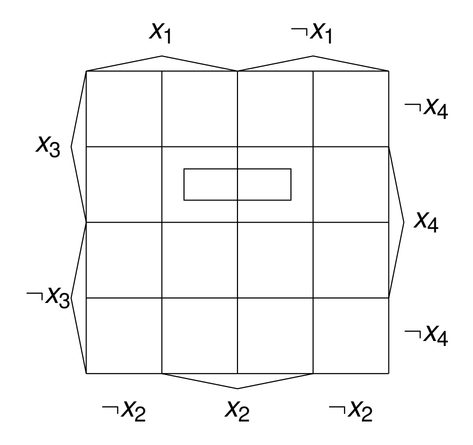
Karnaugh : tous les monômes



Monômes avec 3 variables (exemples) :

$\neg x_1 \wedge \neg x_3 \wedge x_4$

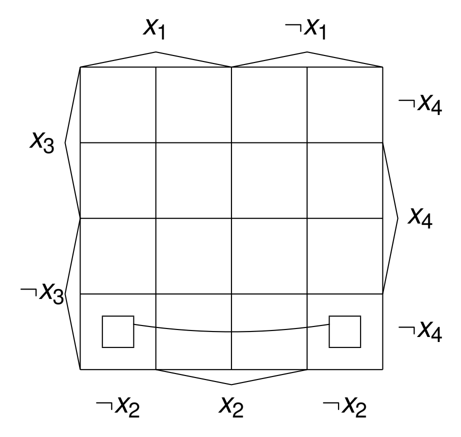
Karnaugh : tous les monômes



Monômes avec 3 variables (exemples) :

$x_2 \wedge x_3 \wedge x_4$

Karnaugh : tous les monômes

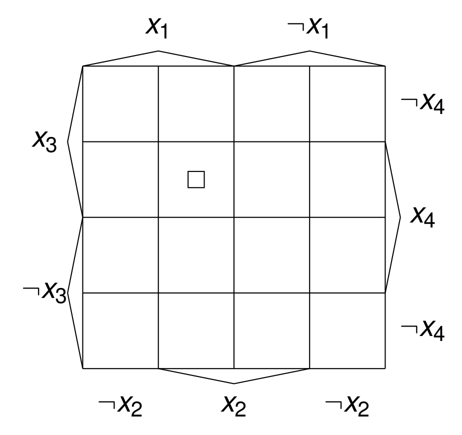


Monômes avec 3 variables (exemples) :

$\neg x_2 \wedge \neg x_3 \wedge \neg x_4$

$\binom{4}{3} \cdot 2^3 = 32$ en total

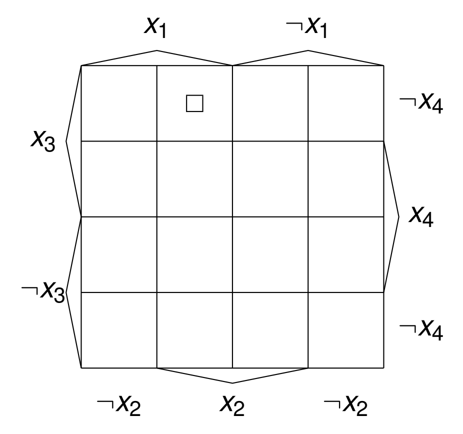
Karnaugh : tous les monômes



Monômes avec 4 variables (exemples) :

$x_1 \wedge x_2 \wedge x_3 \wedge x_4$

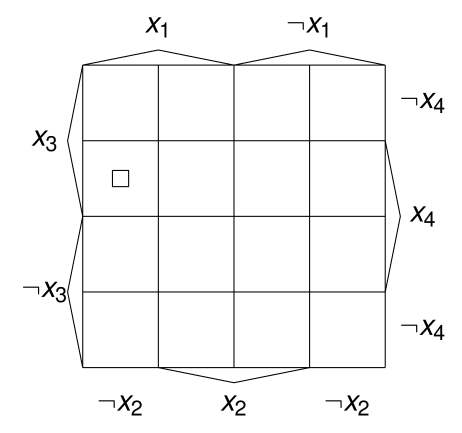
Karnaugh : tous les monômes



Monômes avec 4 variables (exemples) :

$x_1 \wedge x_2 \wedge x_3 \wedge \neg x_4$

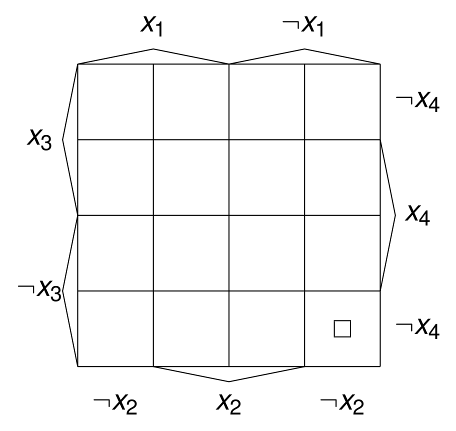
Karnaugh : tous les monômes



Monômes avec 4 variables (exemples) :

$x_1 \wedge \neg x_2 \wedge x_3 \wedge x_4$

Karnaugh : tous les monômes



Monômes avec 4 variables (exemples) :

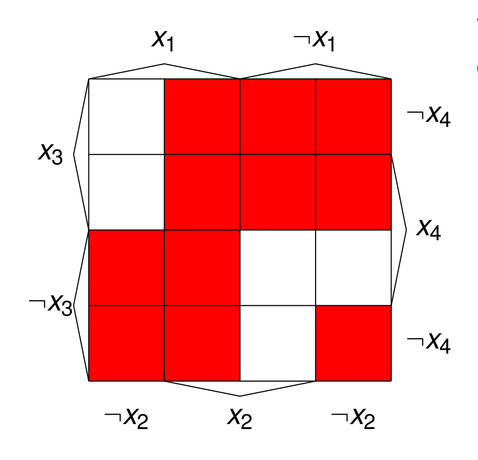
$\neg x_1 \wedge \neg x_2 \wedge \neg x_3 \wedge \neg x_4$

$\binom{4}{4} \cdot 2^4 = 16$ en total

Combien de monômes ?

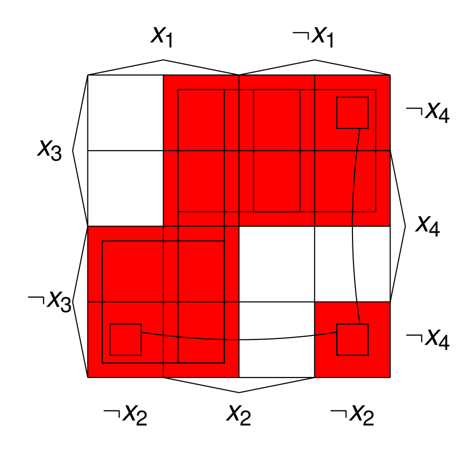
Nous avons compté $8 + 24 + 32 + 16 = 80$ monômes différents. Au même temps, il devrait y avoir $3^4 = 81$ monômes : chacune des 4 variables peut être positive, négative ou absente. Quel monôme avons-nous oublié ?

Exemple d'une fonction (1)



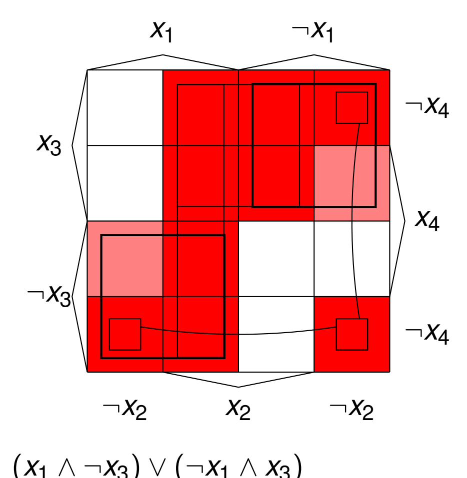
Voilà les points vrais d'une fonction en rouge.

Exemple d'une fonction (1)



Voilà les points vrais d'une fonction en rouge.
Et tous ses 6 monômes maximaux.

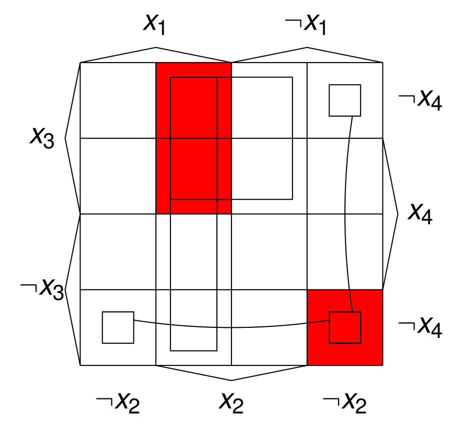
Exemple d'une fonction (1)



Voilà les points vrais d'une fonction en rouge.

Et tous ses 6 monômes maximaux. Les points couverts par un seul monôme maximal en rose avec les monômes centraux correspondants **en gras**. Ils seront de toute façon présents dans toute représentation "simple" et on ne regardera que le reste.

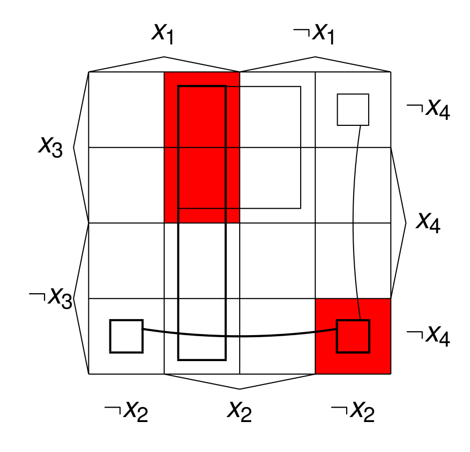
Exemple d'une fonction (1)



$(x_1 \wedge \neg x_3) \vee (\neg x_1 \wedge x_3)$

Voilà les points vrais d'une fonction en rouge.
Et tous ses 6 monômes maximaux.
Les points couverts par un seul monôme maximal en rose avec les monômes centraux correspondants **en gras**. Ils seront de toute façon présents dans toute représentation "simple" et on ne regardera que le reste.
Pour couvrir les points rouges restants, nous avons 2×2 fois le choix.

Exemple d'une fonction (1)

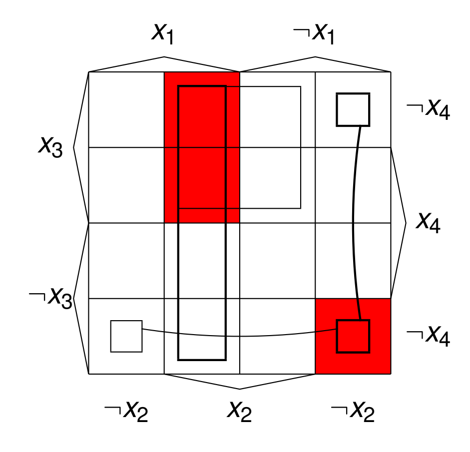


Voilà les points vrais d'une fonction en rouge.
Et tous ses 6 monômes maximaux. Les points couverts par un seul monôme maximal en rose avec les monômes centraux correspondants **en gras**. Ils seront de toute façon présents dans toute représentation “simple” et on ne regardera que le reste.
Pour couvrir les points rouges restants, nous avons 2×2 fois le choix.

$$(x_1 \wedge \neg x_3) \vee (\neg x_1 \wedge x_3) \vee (x_1 \wedge x_2) \vee (\neg x_2 \wedge \neg x_3 \wedge \neg x_4)$$



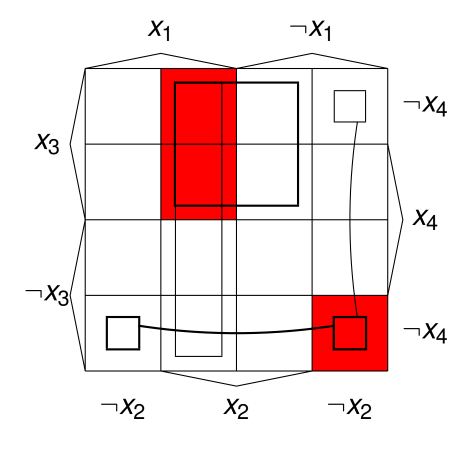
Exemple d'une fonction (1)



Voilà les points vrais d'une fonction en rouge.
Et tous ses 6 monômes maximaux. Les points couverts par un seul monôme maximal en rose avec les monômes centraux correspondants **en gras**. Ils seront de toute façon présents dans toute représentation “simple” et on ne regardera que le reste.
Pour couvrir les points rouges restants, nous avons 2×2 fois le choix.

$$(x_1 \wedge \neg x_3) \vee (\neg x_1 \wedge x_3) \vee (x_1 \wedge x_2) \vee (\neg x_1 \wedge \neg x_2 \wedge \neg x_4)$$

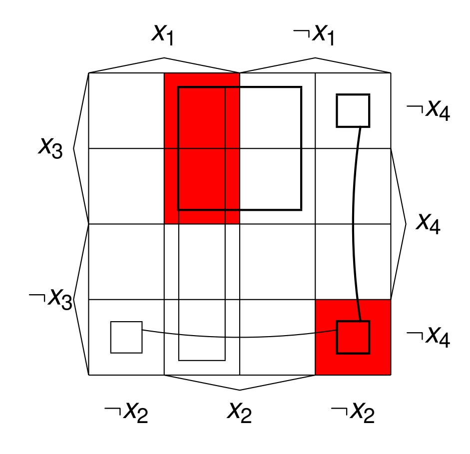
Exemple d'une fonction (1)



Voilà les points vrais d'une fonction en rouge.
Et tous ses 6 monômes maximaux.
Les points couverts par un seul monôme maximal en rose avec les monômes centraux correspondants **en gras**. Ils seront de toute façon présents dans toute représentation "simple" et on ne regardera que le reste.
Pour couvrir les points rouges restants, nous avons 2×2 fois le choix.

$$(x_1 \wedge \neg x_3) \vee (\neg x_1 \wedge x_3) \vee (x_2 \wedge x_3) \vee (\neg x_2 \wedge \neg x_3 \wedge \neg x_4)$$

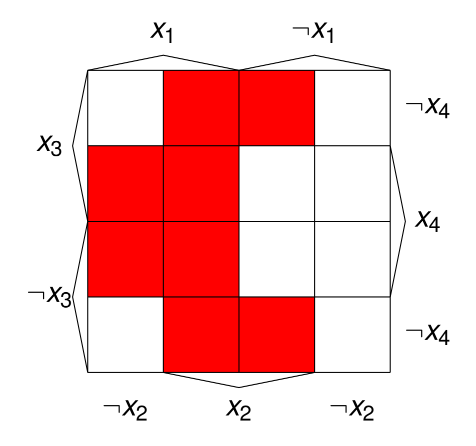
Exemple d'une fonction (1)



Voilà les points vrais d'une fonction en rouge.
Et tous ses 6 monômes maximaux.
Les points couverts par un seul monôme maximal en rose avec les monômes centraux correspondants **en gras**. Ils seront de toute façon présents dans toute représentation "simple" et on ne regardera que le reste.
Pour couvrir les points rouges restants, nous avons 2×2 fois le choix.

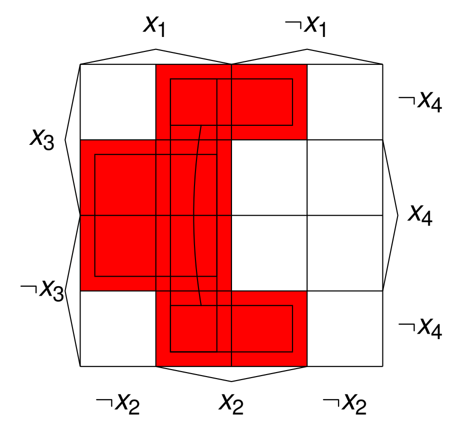
$$(x_1 \wedge \neg x_3) \vee (\neg x_1 \wedge x_3) \vee (x_2 \wedge x_3) \vee (\neg x_1 \wedge \neg x_2 \wedge \neg x_4)$$

Exemple d'une fonction (2)



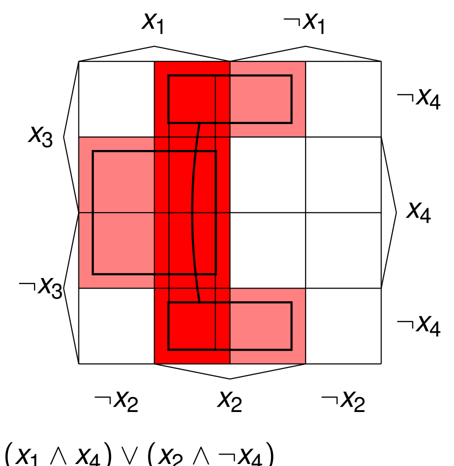
Voilà les points vrais d'une fonction en rouge.

Exemple d'une fonction (2)



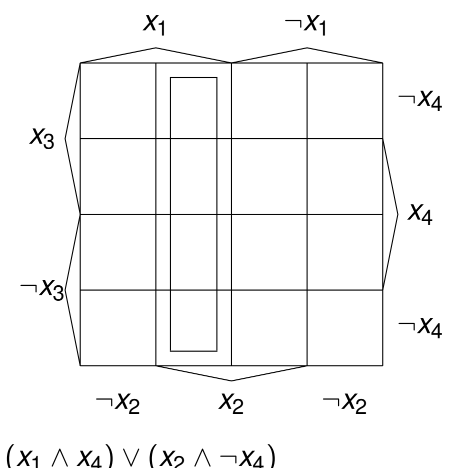
Voilà les points vrais d'une fonction en rouge.
Et tous ses 3 monômes maximaux.

Exemple d'une fonction (2)



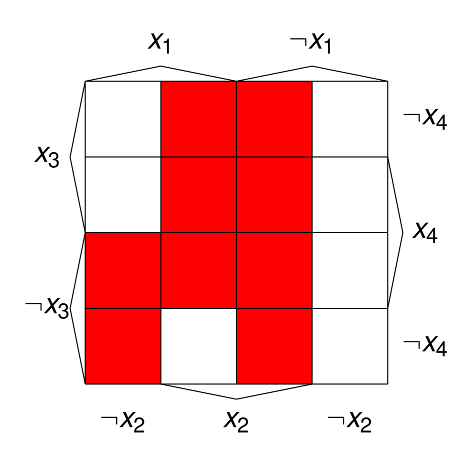
Voilà les points vrais d'une fonction en rouge.
Et tous ses 3 monômes maximaux.
Les points couverts par un seul monôme maximal en rose avec les monômes centraux correspondants **en gras**. Ils seront de toute façon présents dans toute représentation "simple" et on ne regardera que le reste.

Exemple d'une fonction (2)



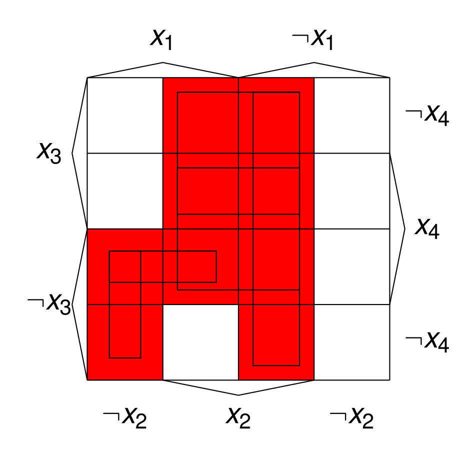
Voilà les points vrais d'une fonction en rouge.
Et tous ses 3 monômes maximaux.
Les points couverts par un seul monôme maximal en rose avec les monômes centraux correspondants **en gras**. Ils seront de toute façon présents dans toute représentation "simple" et on ne regardera que le reste.
Mais il ne reste rien !

Exemple d’une fonction (3)



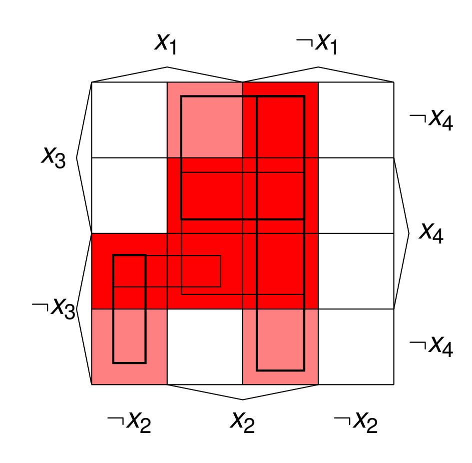
Voilà les points vrais d’une fonction en rouge.

Exemple d'une fonction (3)



Voilà les points vrais d'une fonction en rouge.
Et tous ses 5 monômes maximaux.

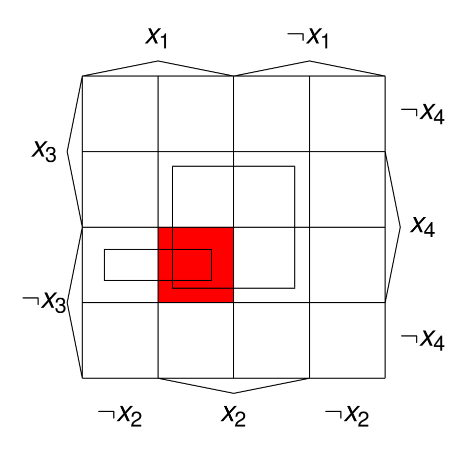
Exemple d'une fonction (3)



Voilà les points vrais d'une fonction en rouge.
Et tous ses 5 monômes maximaux.
Les points couverts par un seul monôme maximal en rose avec les monômes centraux correspondants **en gras**. Ils seront de toute façon présents dans toute représentation "simple" et on ne regardera que le reste.

$$(x_1 \wedge \neg x_2 \wedge \neg x_3) \vee (x_2 \wedge x_3) \vee (\neg x_1 \wedge x_2) \ldots$$

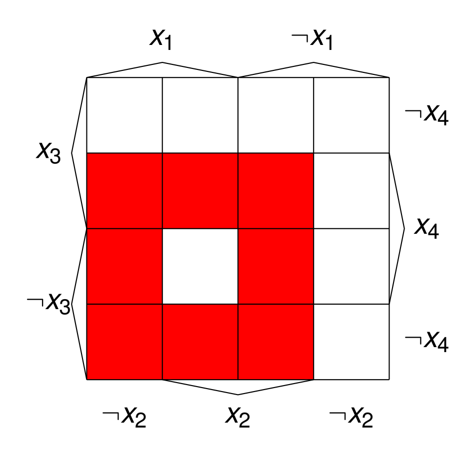
Exemple d'une fonction (3)



Voilà les points vrais d'une fonction en rouge.
Et tous ses 5 monômes maximaux.
Les points couverts par un seul monôme maximal en rose avec les monômes centraux correspondants **en gras**. Ils seront de toute façon présents dans toute représentation "simple" et on ne regardera que le reste.
Pour couvrir le point rouge restant, nous avons 2 fois le choix, mais un choix est clairement préférable ...

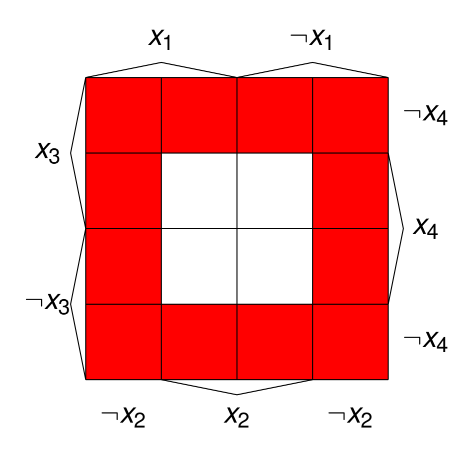
$$(x_1 \wedge \neg x_2 \wedge \neg x_3) \vee (x_2 \wedge x_3) \vee (\neg x_1 \wedge x_2) \ldots$$

Exemple d'une fonction (4)



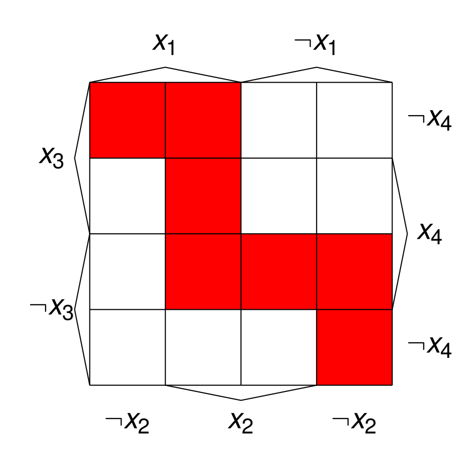
Aucun monôme maximal (il y en a 8) n'est central !

Exemple d'une fonction (5)



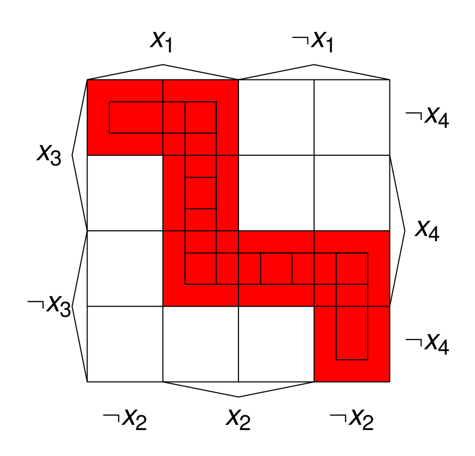
Tous les monômes maximaux (il y en a 2) sont centraux !

Exemple d'une fonction (6)



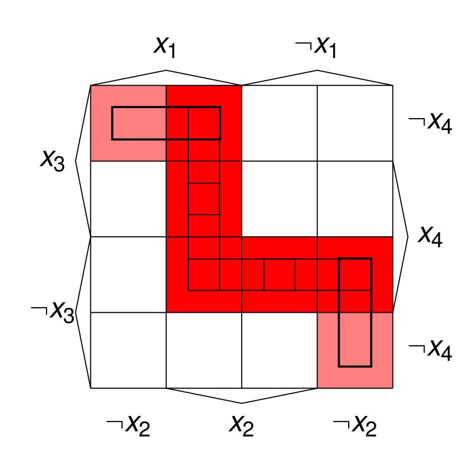
Voilà les points vrais d'une fonction en rouge.

Exemple d'une fonction (6)



Voilà les points vrais d'une fonction en rouge.
Et tous ses 6 monômes maximaux.

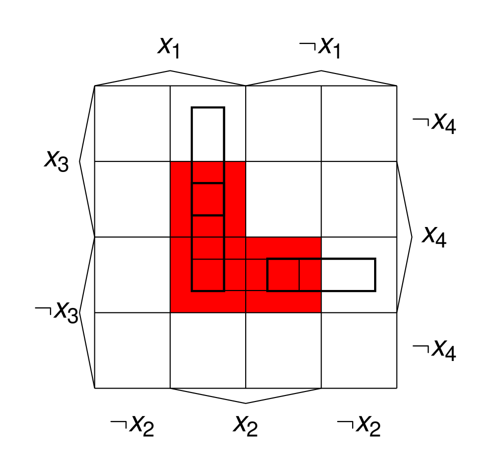
Exemple d'une fonction (6)



Voilà les points vrais d'une fonction en rouge.
Et tous ses 6 monômes maximaux.
Les points couverts par un seul monôme maximal en rose avec les monômes centraux correspondants **en gras**. Ils seront de toute façon présents dans toute représentation "simple" et on ne regardera que le reste.

$$(x_1 \wedge x_3 \wedge \neg x_4) \vee (\neg x_1 \wedge \neg x_2 \wedge \neg x_3) \ldots$$

Exemple d'une fonction (6)



Voilà les points vrais d'une fonction en rouge.

Et tous ses 6 monômes maximaux. Les points couverts par un seul monôme maximal en rose avec les monômes centraux correspondants **en gras**. Ils seront de toute façon présents dans toute représentation "simple" et on ne regardera que le reste.

Pour couvrir les points rouges restants, nous avons 4 monômes à disposition, et un choix naïf peut mener à un résultat sous-optimal. Débrouillez-vous !

$(x_1 \wedge x_3 \wedge \neg x_4) \vee (\neg x_1 \wedge \neg x_2 \wedge \neg x_3) \ldots$

Méthode de Karnaugh (pour $n = 4$)

Soit f une fonction donnée en formule canonique.

1. Marquez les points vrais de la fonction en rouge dans un diagramme de Karnaugh.
2. Identifiez tous les monômes maximaux, en commençant par les monômes à 1 variable et passant vers les monômes à 4 variables.
3. Identifiez les points qui ne sont couverts que par un seul monôme et les monômes correspondants (centraux). Tous ces monômes feront de toute façon partie de la formule “simple”.
4. Éliminez les monômes centraux et tous les points couverts par ceux-ci du diagramme.
5. Choisissez d’autres monômes pour couvrir les points restants.



Méthode de Karnaugh : Commentaires

- Si vous pensez que cette déscription est trop vague : elle et bel et bien plus précise que celle du livre de Marchand !
- Pour le point 5, on voit clairement qu'on peut s'y prendre plus ou moins intelligemment, mais nous n'abordons pas cette question ici.
- Ce n'est pas trop surprenant qu'une méthode graphique et qui est censée marcher bien pour $n \leq 4$ n'ait pas de déscription rigoureuse.
- Il y a d'autres méthodes, par exemple celle de Quine.

Méthode de Karnaugh : Exercices

Mettez-vous à trois :

- Arthur invente une fonction Booléenne à 4 variables en marquant quelques cases en rouge dans un diagramme de Karnaugh.
- Bianca applique la méthode de Karnaugh pour trouver une formule (disjonction de monômes) simple.
- Clément dessine la fonction de cette formule dans un diagramme de Karnaugh vierge.

Ensemble, vérifiez que la fonction de départ est bien identique à celle du résultat.

Plan

Plan

		Lo. prop.	Lo. prédicats	...
Syntaxe		✔		
Sémantique		✔		
Modélisation		✔		
Méth. preuve	• Déd. nat.	☞		
	• Tableaux			
	• Résolution			

Introduction

On se souvient du concept de conséquence logique $H \models C$. Comment on décide $H \models C$?

Introduction

On se souvient du concept de conséquence logique $H \models C$. Comment on décide $H \models C$? On l'a fait avec des tables de vérité.
Pas satisfaisant pour des tâches exigeant un détail du raisonnement (ou explication) qui mène de H à C

- Diagnostic médical
- Diagnostic de panne
- Tuteur électronique
- Agent artificiel intelligent

Nous allons étudier une méthode plus “directe” . . .

Conséquence et Dérivabilité

Conséquence : $\{H_1, \ldots, H_n\} \models C$

- une notion sémantique
- définie à l'aide d'interprétations :
  toute interprétation qui satisfait $\{H_1, \ldots, H_n\}$ satisfait aussi C

Conséquence et Dérivabilité

Conséquence : $\{H_1, \ldots, H_n\} \models C$

- une notion sémantique
- définie à l'aide d'interprétations : toute interprétation qui satisfait $\{H_1, \ldots, H_n\}$ satisfait aussi C

Dérivabilité : $\{H_1, \ldots, H_n\} \vdash C$

- une notion syntaxique
- relative à un calcul (ici, déduction naturelle) : avec les règles du calcul, on peut déduire C à partir des hypothèses $\{H_1, \ldots, H_n\}$

Conséquence et Dérivabilité

Conséquence : $\{H_1, \ldots, H_n\} \models C$

- une notion sémantique
- définie à l'aide d'interprétations :
  toute interprétation qui satisfait $\{H_1, \ldots, H_n\}$ satisfait aussi C

Dérivabilité : $\{H_1, \ldots, H_n\} \vdash C$

- une notion syntaxique
- relative à un calcul (ici, déduction naturelle) : avec les règles du calcul, on peut déduire C à partir des hypothèses $\{H_1, \ldots, H_n\}$

Critères pour un “bon” calcul :

- Correction : si $\{H_1, \ldots, H_n\} \vdash C$, alors $\{H_1, \ldots, H_n\} \models C$
- Complétude : si $\{H_1, \ldots, H_n\} \models C$, alors $\{H_1, \ldots, H_n\} \vdash C$

Conséquence et Dérivabilité

Conséquence : $\{H_1, \dots, H_n\} \models C$

- une notion sémantique
- définie à l'aide d'interprétations :
  toute interprétation qui satisfait $\{H_1, \dots, H_n\}$ satisfait aussi C

Dérivabilité : $\{H_1, \dots, H_n\} \vdash C$

- une notion syntaxique
- relative à un calcul (ici, déduction naturelle) : avec les règles du calcul, on peut déduire C à partir des hypothèses $\{H_1, \dots, H_n\}$

Critères pour un “bon” calcul :

- Correction : si $\{H_1, \dots, H_n\} \vdash C$, alors $\{H_1, \dots, H_n\} \models C$
- Complétude : si $\{H_1, \dots, H_n\} \models C$, alors $\{H_1, \dots, H_n\} \vdash C$

Cas particulier : $\models C$ (validité) vs. $\vdash C$ (prouvabilité).



Déduction naturelle : exemple (1)

Exemple de raisonnement “naturel”

Quelques propositions :

1. Quand il neige, il fait froid : $(N \longrightarrow F)$
2. Quand il y a du verglas, il fait froid : $(V \longrightarrow F)$
3. Il neige ou il y a du verglas $(N \vee V)$
4. En été, il ne fait pas froid $(E \longrightarrow \neg F)$
5. Donc, on n’est pas été : $\neg E$

Déduction naturelle : exemple (1)

Exemple de raisonnement “naturel”

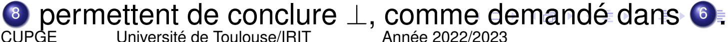
Quelques propositions :

1. Quand il neige, il fait froid : $(N \longrightarrow F)$
2. Quand il y a du verglas, il fait froid : $(V \longrightarrow F)$
3. Il neige ou il y a du verglas $(N \vee V)$
4. En été, il ne fait pas froid $(E \longrightarrow \neg F)$
5. Donc, on n’est pas été : $\neg E$

Dérivation de (5) à partir de (1) . . . (4) :

6. Pour montrer (5), supposons E, et dérivons une contradiction $(\perp)$
7. Distinction de cas (avec (3)) :
    1. Soit N. Alors, avec (1), on a F.
    2. Soit V. Alors, avec (2), on a F.

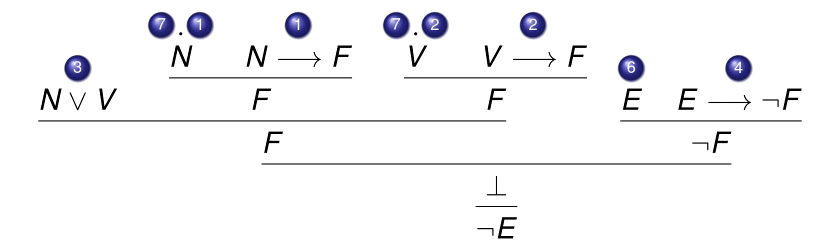
   Donc, de (1), (2), (3) on peut conclure F.
8. Avec (6) et (4), inférer $\neg F$.
9. (7) et (8) permettent de conclure $\perp$, comme demandé dans (6).





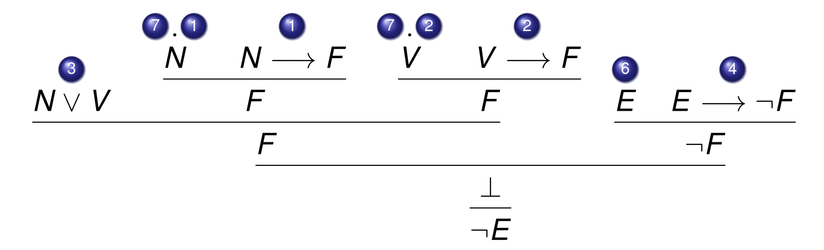
Déduction naturelle : exemple (2)

Arbre de dérivation :



Déduction naturelle : exemple (2)

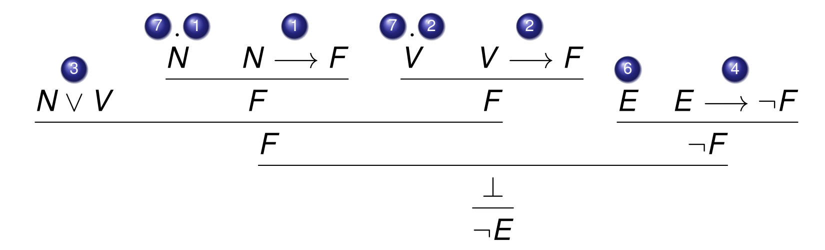
Arbre de dérivation :



Nous dirons : Sous les hypothèses ❶ . . . ❹, on peut déduire ou dériver la conclusion ❺.

Déduction naturelle : exemple (2)

Arbre de dérivation :



Nous dirons : Sous les hypothèses ❶ . . . ❹, on peut déduire ou dériver la conclusion ❺.
Ce fait est exprimé par le jugement
$\{N \longrightarrow F, V \longrightarrow F, N \vee V, E \longrightarrow \neg F\} \vdash \neg E$

Histoire : Hilbert



Hilbert (1862 - 1943)

- Contributions essentielles aux fondements de la mathématique :
  - Axiomatisation de la géométrie Euclidienne
  - ... et dans la suite : axiomatisation de la mathématique
- “Programme de Hilbert” :
  - Trouver un système d’axiomes et règles de déduction qui assurent la consistance de la mathématique
  - (mis à mal par les résultats de Gödel)

Histoire : Gentzen



Gentzen (1909 - 1945)

- Développement de deux calculs (1934) :
  - Déduction naturelle, pour rendre l'axiomatisation de Hilbert plus utilisable
  - Calcul des séquents : une procédure effective de preuve
  - Les deux calculs sont équivalents ("élimination des coupures")
- Méthode des tableaux :
  - Variante du calcul des séquents
  - ...introduite vers 1955 par E.W.Beth

Voir article The Development of Proof Theory



Déduction naturelle : une règle générale

Dans tous les cas, nous aurons toujours la règle suivante :
Axiome :

$$\frac{A \in \Gamma}{\Gamma \vdash A}\ (Ax)$$

Notation : Dans un arbre de dérivation, on n'écrit pas explicitement la précondition $A \in \Gamma$. Souvent, on supprime même l'entière application de la règle (Ax) dans la présentation.

Déduction naturelle : un exemple abstrait

Nous avons déjà donné un exemple intuitif (neige, verglas . . .).

Déduction naturelle : un exemple abstrait

Nous avons déjà donné un exemple intuitif (neige, verglas . . .).
Pour mieux apprécier que la déduction est un processus entièrement mécanique et que nous ne pouvons pas utiliser notre intuition sémantique comme bon nous semble, il est utile de présenter un exemple abstrait, sans aucune intuition.

Déduction naturelle : un exemple abstrait

Nous avons déjà donné un exemple intuitif (neige, verglas ...).
Pour mieux apprécier que la déduction est un processus entièrement mécanique et que nous ne pouvons pas utiliser notre intuition sémantique comme bon nous semble, il est utile de présenter un exemple abstrait, sans aucune intuition.

- Langage $\mathcal{L} = \{\heartsuit, \clubsuit, \spadesuit, \diamondsuit\}$.

Déduction naturelle : un exemple abstrait

Nous avons déjà donné un exemple intuitif (neige, verglas . . .).
Pour mieux apprécier que la déduction est un processus entièrement mécanique et que nous ne pouvons pas utiliser notre intuition sémantique comme bon nous semble, il est utile de présenter un exemple abstrait, sans aucune intuition.

- Langage $\mathcal{L} = \{\heartsuit, \clubsuit, \spadesuit, \diamondsuit\}$.
- Système déductif donné par les règles :

$$\frac{\Gamma \vdash \diamondsuit}{\Gamma \vdash \clubsuit}\ (1) \qquad \frac{\Gamma \vdash \diamondsuit}{\Gamma \vdash \spadesuit}\ (2) \qquad \frac{\Gamma \vdash \clubsuit \quad \Gamma \vdash \spadesuit}{\Gamma \vdash \heartsuit}\ (3) \qquad \frac{\Gamma, \diamondsuit \vdash \heartsuit}{\Gamma \vdash \heartsuit}\ (4)$$

Déduction naturelle : un exemple abstrait

Nous avons déjà donné un exemple intuitif (neige, verglas . . .).
Pour mieux apprécier que la déduction est un processus entièrement mécanique et que nous ne pouvons pas utiliser notre intuition sémantique comme bon nous semble, il est utile de présenter un exemple abstrait, sans aucune intuition.

- Langage $\mathcal{L} = \{\heartsuit, \clubsuit, \spadesuit, \diamondsuit\}$.
- Système déductif donné par les règles :

$$\frac{\Gamma \vdash \diamondsuit}{\Gamma \vdash \clubsuit}\ (1) \qquad \frac{\Gamma \vdash \diamondsuit}{\Gamma \vdash \spadesuit}\ (2) \qquad \frac{\Gamma \vdash \clubsuit \quad \Gamma \vdash \spadesuit}{\Gamma \vdash \heartsuit}\ (3) \qquad \frac{\Gamma, \diamondsuit \vdash \heartsuit}{\Gamma \vdash \heartsuit}\ (4)$$

- (1) : si vous avez un $\diamondsuit$ je vous donne un $\clubsuit$

Déduction naturelle : un exemple abstrait

Nous avons déjà donné un exemple intuitif (neige, verglas ...).
Pour mieux apprécier que la déduction est un processus entièrement mécanique et que nous ne pouvons pas utiliser notre intuition sémantique comme bon nous semble, il est utile de présenter un exemple abstrait, sans aucune intuition.

- Langage $\mathcal{L} = \{\heartsuit, \clubsuit, \spadesuit, \diamondsuit\}$.
- Système déductif donné par les règles :

$$\frac{\Gamma \vdash \diamondsuit}{\Gamma \vdash \clubsuit}\ (1) \qquad \frac{\Gamma \vdash \diamondsuit}{\Gamma \vdash \spadesuit}\ (2) \qquad \frac{\Gamma \vdash \clubsuit \quad \Gamma \vdash \spadesuit}{\Gamma \vdash \heartsuit}\ (3) \qquad \frac{\Gamma, \diamondsuit \vdash \heartsuit}{\Gamma \vdash \heartsuit}\ (4)$$

- (1) : si vous avez un $\diamondsuit$ je vous donne un $\clubsuit$
- (3) : si vous avez un $\clubsuit$ et un $\spadesuit$ je vous donne un $\heartsuit$

Déduction naturelle : un exemple abstrait

Nous avons déjà donné un exemple intuitif (neige, verglas . . .).
Pour mieux apprécier que la déduction est un processus entièrement mécanique et que nous ne pouvons pas utiliser notre intuition sémantique comme bon nous semble, il est utile de présenter un exemple abstrait, sans aucune intuition.

- Langage $\mathcal{L} = \{\heartsuit, \clubsuit, \spadesuit, \diamondsuit\}$.
- Système déductif donné par les règles :

$$\frac{\Gamma \vdash \diamondsuit}{\Gamma \vdash \clubsuit}\ (1) \qquad \frac{\Gamma \vdash \diamondsuit}{\Gamma \vdash \spadesuit}\ (2) \qquad \frac{\Gamma \vdash \clubsuit \quad \Gamma \vdash \spadesuit}{\Gamma \vdash \heartsuit}\ (3) \qquad \frac{\Gamma, \diamondsuit \vdash \heartsuit}{\Gamma \vdash \heartsuit}\ (4)$$

- (1) : si vous avez un ♦ je vous donne un ♣
- (3) : si vous avez un ♣ et un ♠ je vous donne un ♥
- (4) : si vous savez obtenir un ♥ à partir d'un ♦, je vous donne un ♥ (vous pouvez emprunter une carte, mais il faudra la rendre !)

Preuve de ♥

Les règles :

$$\frac{\Gamma \vdash \blacklozenge}{\Gamma \vdash \clubsuit}\ (1) \quad \frac{\Gamma \vdash \blacklozenge}{\Gamma \vdash \spadesuit}\ (2) \quad \frac{\Gamma \vdash \clubsuit \quad \Gamma \vdash \spadesuit}{\Gamma \vdash \heartsuit}\ (3) \quad \frac{\Gamma, \blacklozenge \vdash \heartsuit}{\Gamma \vdash \heartsuit}\ (4)$$

Ax

La preuve :

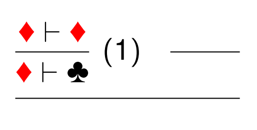


Preuve de ♥

Les règles :

$$\frac{\Gamma \vdash \blacklozenge}{\Gamma \vdash \clubsuit}\ (1) \qquad \frac{\Gamma \vdash \blacklozenge}{\Gamma \vdash \spadesuit}\ (2) \qquad \frac{\Gamma \vdash \clubsuit \quad \Gamma \vdash \spadesuit}{\Gamma \vdash \heartsuit}\ (3) \qquad \frac{\Gamma, \blacklozenge \vdash \heartsuit}{\Gamma \vdash \heartsuit}\ (4)$$

La preuve :



Ax

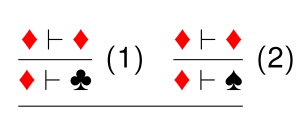
On applique (1).

Preuve de ♥

Les règles :

$$\frac{\Gamma \vdash \blacklozenge}{\Gamma \vdash \clubsuit}\ (1) \quad \frac{\Gamma \vdash \blacklozenge}{\Gamma \vdash \spadesuit}\ (2) \quad \frac{\Gamma \vdash \clubsuit \quad \Gamma \vdash \spadesuit}{\Gamma \vdash \heartsuit}\ (3) \quad \frac{\Gamma, \blacklozenge \vdash \heartsuit}{\Gamma \vdash \heartsuit}\ (4)$$

La preuve :



Ax
On applique (1).
De la même façon avec (2).

Preuve de ♥

Les règles :

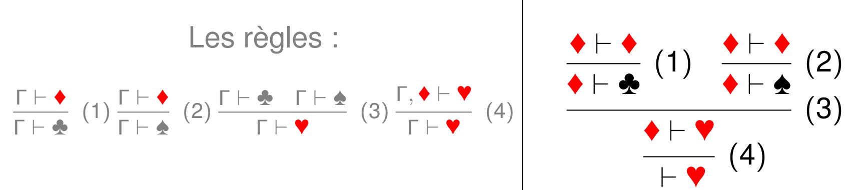
$$\frac{\Gamma \vdash \blacklozenge}{\Gamma \vdash \clubsuit}\ (1) \qquad \frac{\Gamma \vdash \blacklozenge}{\Gamma \vdash \spadesuit}\ (2) \qquad \frac{\Gamma \vdash \clubsuit \quad \Gamma \vdash \spadesuit}{\Gamma \vdash \heartsuit}\ (3) \qquad \frac{\Gamma, \blacklozenge \vdash \heartsuit}{\Gamma \vdash \heartsuit}\ (4)$$

La preuve :

$$\cfrac{\cfrac{\blacklozenge \vdash \blacklozenge}{\blacklozenge \vdash \clubsuit}\ (1) \qquad \cfrac{\blacklozenge \vdash \blacklozenge}{\blacklozenge \vdash \spadesuit}\ (2)}{\cfrac{\blacklozenge \vdash \heartsuit}{}}\ (3)$$

Ax
On applique (1).
De la même façon avec (2).
On applique (3).

Preuve de ♥



Ax
On applique (1).
De la même façon avec (2).
On applique (3).
On applique (4). Notez que l'hypothèse ♦ a disparu. On appelle une telle dérivation (sans hypothèses) une preuve.

Une dérivation avec hypothèses

Autre système de règles (sans (2) !) :

$$\frac{\Gamma \vdash \diamondsuit}{\Gamma \vdash \clubsuit}\ (1) \qquad \frac{\Gamma \vdash \clubsuit \quad \Gamma \vdash \spadesuit}{\Gamma \vdash \heartsuit}\ (3) \qquad \frac{\Gamma, \diamondsuit \vdash \heartsuit}{\Gamma \vdash \heartsuit}\ (4)$$

La dérivation :

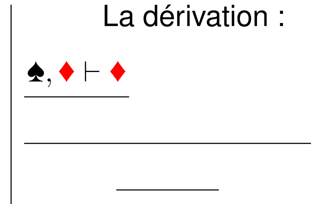
Sauriez-vous obtenir un $\heartsuit$ avec seulement des $\spadesuit$?

Une dérivation avec hypothèses

Autre système de règles (sans (2) !) :

$$\frac{\Gamma \vdash \blacklozenge}{\Gamma \vdash \clubsuit}\ (1) \qquad \frac{\Gamma \vdash \clubsuit \quad \Gamma \vdash \spadesuit}{\Gamma \vdash \heartsuit}\ (3) \qquad \frac{\Gamma, \blacklozenge \vdash \heartsuit}{\Gamma \vdash \heartsuit}\ (4)$$

Par axiome.



Sauriez-vous obtenir un ♥ avec seulement des ♠ ?

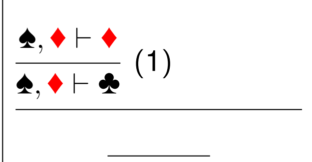
Une dérivation avec hypothèses

Autre système de règles (sans (2) !) :

$$\frac{\Gamma \vdash \diamondsuit}{\Gamma \vdash \clubsuit}\ (1) \qquad \frac{\Gamma \vdash \clubsuit \quad \Gamma \vdash \spadesuit}{\Gamma \vdash \heartsuit}\ (3) \qquad \frac{\Gamma, \diamondsuit \vdash \heartsuit}{\Gamma \vdash \heartsuit}\ (4)$$

Par axiome.
On applique (1).

La dérivation :



$$\frac{\spadesuit, \diamondsuit \vdash \diamondsuit}{\spadesuit, \diamondsuit \vdash \clubsuit}\ (1)$$

Sauriez-vous obtenir un $\heartsuit$ avec seulement des $\spadesuit$?

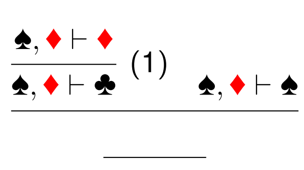
Une dérivation avec hypothèses

Autre système de règles (sans (2) !) :

$$\frac{\Gamma \vdash \blacklozenge}{\Gamma \vdash \clubsuit}\ (1) \qquad \frac{\Gamma \vdash \clubsuit \quad \Gamma \vdash \spadesuit}{\Gamma \vdash \heartsuit}\ (3) \qquad \frac{\Gamma, \blacklozenge \vdash \heartsuit}{\Gamma \vdash \heartsuit}\ (4)$$

Par axiome.
On applique (1).
Par axiome.

La dérivation :



Sauriez-vous obtenir un ♥ avec seulement des ♠ ?

Une dérivation avec hypothèses

Autre système de règles (sans (2) !) :

$$\frac{\Gamma \vdash \diamondsuit}{\Gamma \vdash \clubsuit}\ (1) \qquad \frac{\Gamma \vdash \clubsuit \quad \Gamma \vdash \spadesuit}{\Gamma \vdash \heartsuit}\ (3) \qquad \frac{\Gamma, \diamondsuit \vdash \heartsuit}{\Gamma \vdash \heartsuit}\ (4)$$

Par axiome.
On applique (1).
Par axiome.
On applique (3).

La dérivation :

$$\frac{\dfrac{\spadesuit, \diamondsuit \vdash \diamondsuit}{\spadesuit, \diamondsuit \vdash \clubsuit}\ (1) \qquad \spadesuit, \diamondsuit \vdash \spadesuit}{\spadesuit, \diamondsuit \vdash \heartsuit}\ (3)$$

Sauriez-vous obtenir un $\heartsuit$ avec seulement des $\spadesuit$?

Une dérivation avec hypothèses

Autre système de règles (sans (2) !) :

$$\frac{\Gamma \vdash \blacklozenge}{\Gamma \vdash \clubsuit}\ (1) \qquad \frac{\Gamma \vdash \clubsuit \quad \Gamma \vdash \spadesuit}{\Gamma \vdash \heartsuit}\ (3) \qquad \frac{\Gamma, \blacklozenge \vdash \heartsuit}{\Gamma \vdash \heartsuit}\ (4)$$

La dérivation :

$$\dfrac{\dfrac{\dfrac{\spadesuit, \blacklozenge \vdash \blacklozenge}{\spadesuit, \blacklozenge \vdash \clubsuit}\ (1) \qquad \spadesuit, \blacklozenge \vdash \spadesuit}{\spadesuit, \blacklozenge \vdash \heartsuit}\ (3)}{\spadesuit \vdash \heartsuit}\ (4)$$

Sauriez-vous obtenir un ♥ avec seulement des ♠ ?

Par axiome.
On applique (1).
Par axiome.
On applique (3).
On applique (4). Notez que l'hypothèse ♦ a disparu. Nous avons une dérivation de ♥ à partir de ♠.

Règles d'inférence

Une règle

$$\frac{J^1 \quad \dots \quad J^m}{J}$$

est composée de

- 0, 1 ou plusieurs antécédents
- un seul conséquent

Lecture informelle :
"Si tous les antécédents sont prouvables, alors aussi le conséquent"

Chaque J a la forme d'un jugement $\{H_1, \dots, H_n\} \vdash C$
Souvent, l'ensemble d'hypothèses est abrégé par Γ

- On écrit Γ, A pour $\Gamma \cup \{A\}$
- On écrit $\vdash A$ pour $\{\} \vdash A$

Typologie des règles

Pour chaque connecteur, il y a une (éventuellement deux)

- règle(s) d'introduction (connecteur dans le conséquent),
- règle(s) d'élimination (connecteur dans l'antécédent principal),

Typologie des règles : Règles pour $\wedge$

Pour chaque connecteur, il y a une (éventuellement deux)

- règle(s) d'introduction (connecteur dans le conséquent), par exemple $(I\wedge)$
- règle(s) d'élimination (connecteur dans l'antécédent principal), par exemple $(E\wedge_1)$ et $(E\wedge_2)$

- Règle d'introduction :

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \ (I\wedge)$$

- Règles d'élimination :

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \ (E\wedge_1) \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \ (E\wedge_2)$$

Règles pour $\longrightarrow$

- Intro :

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \longrightarrow B} \ (I \longrightarrow)$$

- Elim :

$$\frac{\Gamma \vdash A \longrightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B} \ (E \longrightarrow)$$

Note : $(E \longrightarrow)$ aussi appelée modus ponens

Règles pour ¬

- Intro :

$$\frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A} \ (I\neg)$$

- Elim :

$$\frac{\Gamma \vdash \neg A \qquad \Gamma \vdash A}{\Gamma \vdash \bot} \ (E\neg)$$

Observation ?

Règles pour $\neg$

- Intro :

$$\frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}\ (I\neg)$$

- Elim :

$$\frac{\Gamma \vdash \neg A \qquad \Gamma \vdash A}{\Gamma \vdash \bot}\ (E\neg)$$

Observation ?
Ce sont des cas spéciaux des règles pour $\longrightarrow$, en considérant que $\neg A$ n'est qu'une abréviation pour $A \longrightarrow \bot$.

Règles pour $\neg$

- Intro :

$$\frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A} \; (I\neg)$$

- Elim :

$$\frac{\Gamma \vdash \neg A \qquad \Gamma \vdash A}{\Gamma \vdash \bot} \; (E\neg)$$

Observation ?
Ce sont des cas spéciaux des règles pour $\longrightarrow$, en considérant que $\neg A$ n'est qu'une abréviation pour $A \longrightarrow \bot$.

Exercice : $\vdash \neg(p \wedge q) \longrightarrow \neg(q \wedge p)$

Règles pour $\perp$

- Intro ?



Règles pour $\bot$

- Intro ? Il n'y en a pas ! ! !
- Elim :

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash A}\ (E\bot)$$

Note : $(E\bot)$ aussi appelée ex falso quodlibet ou encore ex contradictione sequitur quodlibet ou encore Principe de Pseudo Scotus (logicien médiéval).

Règles pour $\bot$

- Intro ? Il n'y en a pas !!!
- Elim :

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash A}\ (E\bot)$$

Note : $(E\bot)$ aussi appelée ex falso quodlibet ou encore ex contradictione sequitur quodlibet ou encore Principe de Pseudo Scotus (logicien médiéval).

Exercice : $\vdash \neg(p \longrightarrow q) \longrightarrow \neg p \longrightarrow r$

Règles pour $\vee$ (1)

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ (I\vee_1) \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ (I\vee_2)$$

$$\frac{\Gamma \vdash A \vee B \qquad \Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma \vdash C}\ (E\vee)$$

Note : $(E\vee)$ correspond à une distinction de cas.

Que faire pour les disjonctions ?

Rappel : Quand vous construisez une dérivation du bas vers le haut et le jugement actuel est ...

- $\ldots \vdash \phi \longrightarrow \psi$, dans 90% (?) des cas c'est une bonne idée d'utiliser ($I \longrightarrow$).
- $\ldots \vdash \phi \wedge \psi$, dans 99% (?) des cas c'est une bonne idée d'utiliser ($I\wedge$).

Que faire pour les disjonctions ?

Rappel : Quand vous construisez une dérivation du bas vers le haut et le jugement actuel est . . .

- $\ldots \vdash \phi \longrightarrow \psi$, dans 90% (?) des cas c'est une bonne idée d'utiliser $(I \longrightarrow)$.
- $\ldots \vdash \phi \wedge \psi$, dans 99% (?) des cas c'est une bonne idée d'utiliser $(I\wedge)$.

Alors on serait tenté de penser :

> *Quand je construis une dérivation du bas vers le haut et le jugement actuel est* $\ldots \vdash \phi \vee \psi$*, alors je vais utiliser* $(I\vee_1)$ *ou peut-être* $(I\vee_2)$*.*

Que faire pour les disjonctions ?

Rappel : Quand vous construisez une dérivation du bas vers le haut et le jugement actuel est ...

- $\ldots \vdash \phi \longrightarrow \psi$, dans 90% (?) des cas c'est une bonne idée d'utiliser ($I \longrightarrow$).
- $\ldots \vdash \phi \wedge \psi$, dans 99% (?) des cas c'est une bonne idée d'utiliser ($I\wedge$).

Alors on serait tenté de penser :

> *Quand je construis une dérivation du bas vers le haut et le jugement actuel est* $\ldots \vdash \phi \vee \psi$, *alors je vais utiliser* ($I\vee_1$) *ou peut-être* ($I\vee_2$).

C'est presque toujours une très mauvaise idée ! ! !

Que faire pour les disjonctions ? (2)

En fait : quand vous construisez une dérivation du bas vers le haut et vous rencontrez le jugement $\ldots \vdash \phi \vee \psi$ **pour la première fois**, presque toujours votre contexte (ce qui est à gauche de $\vdash$) est trop faible pour dériver $\phi \vee \psi$ “directement” en utilisant $(I\vee_1)$ ou $(I\vee_2)$.

Que faire pour les disjonctions ? (2)

En fait : quand vous construisez une dérivation du bas vers le haut et vous rencontrez le jugement $\ldots \vdash \phi \lor \psi$ **pour la première fois**, presque toujours votre contexte (ce qui est à gauche de $\vdash$) est trop faible pour dériver $\phi \lor \psi$ "directement" en utilisant ($I\lor_1$) ou ($I\lor_2$). Vous devez renforcer le contexte.

Que faire pour les disjonctions ? (2)

En fait : quand vous construisez une dérivation du bas vers le haut et vous rencontrez le jugement $\ldots \vdash \phi \vee \psi$ **pour la première fois**, presque toujours votre contexte (ce qui est à gauche de $\vdash$) est trop faible pour dériver $\phi \vee \psi$ "directement" en utilisant $(I\vee_1)$ ou $(I\vee_2)$.
Vous devez renforcer le contexte.
Mais comment ?

Que faire pour les disjonctions ? (2)

En fait : quand vous construisez une dérivation du bas vers le haut et vous rencontrez le jugement $\ldots \vdash \phi \vee \psi$ **pour la première fois**, presque toujours votre contexte (ce qui est à gauche de $\vdash$) est trop faible pour dériver $\phi \vee \psi$ “directement” en utilisant $(I\vee_1)$ ou $(I\vee_2)$.
Vous devez renforcer le contexte.
Mais comment ?
Le principe qui prévaut est le suivant :

> *Quand le jugement a la forme* $\ldots \alpha \vee \beta \ldots \vdash \ldots$*, c.-à-d.* $\alpha \vee \beta$ *apparaît* ***à gauche*** *de* $\vdash$*, essayez d'utiliser* $(E\vee)$*.*

Que faire pour les disjonctions ? (2)

En fait : quand vous construisez une dérivation du bas vers le haut et vous rencontrez le jugement $\ldots \vdash \phi \vee \psi$ **pour la première fois**, presque toujours votre contexte (ce qui est à gauche de $\vdash$) est trop faible pour dériver $\phi \vee \psi$ “directement” en utilisant $(I\vee_1)$ ou $(I\vee_2)$.
Vous devez renforcer le contexte.
Mais comment ?
Le principe qui prévaut est le suivant :

> *Quand le jugement a la forme* $\ldots \alpha \vee \beta \ldots \vdash \ldots$*, c.-à-d.* $\alpha \vee \beta$ *apparaît* ***à gauche*** *de* $\vdash$*, essayez d'utiliser* $(E\vee)$*.*

En résumé :

> *Quand vous rencontrez* $\ldots \vdash \phi \vee \psi$ *(pour la première fois), ne faites pas* $(I\vee_1)$ *ou* $(I\vee_2)$*, mais essayez plutôt de faire* $(E\vee)$*.*

Cela rompt avec le principe appliqué pour $\wedge$ et $\longrightarrow$ et paraît bizarre à première vue !

Exemple

Soit $\Gamma = p \vee q \vee r$
$\Gamma_p = p \vee q \vee r, p$
$\Gamma_{qr} = p \vee q \vee r, q \vee r$
$\Gamma_q = p \vee q \vee r, q \vee r, q$
$\Gamma_r = p \vee q \vee r, q \vee r, r$

$$\dfrac{\dfrac{}{\Gamma \vdash p \vee q \vee r}(Ax) \quad \dfrac{\dfrac{\dfrac{}{\Gamma_p \vdash p}(Ax)}{\Gamma_p \vdash (p \vee q)}(I\vee_1)}{\Gamma_p \vdash (p \vee q) \vee r}(I\vee_1) \quad \dfrac{\dfrac{}{\Gamma_{qr} \vdash q \vee r}(Ax) \quad \dfrac{\dfrac{\dfrac{}{\Gamma_q \vdash q}(Ax)}{\Gamma_q \vdash (p \vee q)}(I\vee_2)}{\Gamma_q \vdash (p \vee q) \vee r}(I\vee_1) \quad \dfrac{\dfrac{}{\Gamma_r \vdash r}(Ax)}{\Gamma_r \vdash (p \vee q) \vee r}(I\vee_2)}{\Gamma_{qr} \vdash (p \vee q) \vee r}(E\vee)}{\Gamma \vdash (p \vee q) \vee r}(E\vee)$$

(ligne horizontale en bas pas assez large pour problème technique inconnu)

Remarques

- On voit comme les règles ($I\vee_1$) et ($I\vee_2$) ne sont appliquées qu'une fois le contexte étant suffisamment fort.
- Pour la règle ($E\vee$), il faut **deviner** quelles formules mettre pour A et B. Le principe (et cela n'est pas nouveau pour vous) : on choisit une disjonction qui apparaît à gauche du $\vdash$ (éventuellement dans une sous-formule).

Encore une fois : Exemple introductoire

Soit $\Gamma = \{N \longrightarrow F, V \longrightarrow F, N \vee V, E \longrightarrow \neg F\}$, $\Gamma' = \Gamma \cup \{E\}$

Arbres de dérivation :

Soit $[A_1] =$

$$\dfrac{\Gamma' \vdash N \vee V \qquad \dfrac{\Gamma', N \vdash N \longrightarrow F \qquad \Gamma', N \vdash N}{\Gamma', N \vdash F} \qquad \dfrac{\Gamma', V \vdash V \longrightarrow F \qquad \Gamma', V \vdash V}{\Gamma', V \vdash F}}{\Gamma' \vdash F}$$

Alors :

$$\dfrac{\dfrac{\dfrac{\Gamma' \vdash E \longrightarrow \neg F \qquad \Gamma' \vdash E}{\Gamma' \vdash \neg F} \qquad [A_1]}{\Gamma' \vdash \bot}}{\Gamma \vdash \neg E}$$

Exercices

Pour les exercices, envoyez/uploadez un scan, une photo, un pdf si vous disposez d'un outil sophistiqué pour afficher des arbres de dérivation, ou un “graphique ASCII” improvisé du genre

```
   p,q |- q     p,q |- p
- - - - - - - - - - - - -  (I/\)
     p,q |- q /\ p
```

Essayez d'abréger les contextes intelligemment : dès que vous obtenez un contexte qui risque d'apparaître plusieurs fois, introduisez une abréviation.
Pour chaque exercice à forum, veuillez ouvrir un nouveau sujet sur Moodle si vous y répondez.

Exercices I

Question

Prouvez le jugement $\vdash p \vee q \longrightarrow q \vee p$ par déduction naturelle.

Question

Pareil pour $r \longrightarrow p \vee q \vdash r \longrightarrow q \vee p$.

Exercices II

Question

Pareil pour $p \vee q \longrightarrow r \vdash q \vee p \longrightarrow r$.

Devoir à la maison / TD

Pareil pour $\neg(p \vee q) \vdash \neg p \wedge \neg q$

Devoir à la maison / TD

Pareil pour $\neg p \wedge \neg q \vdash \neg(p \vee q)$.

Devoir à la maison / TD

Pareil pour $\neg p \vee \neg q \vdash \neg(p \wedge q)$.

Logique intuitionniste et classique

Nous avons maintenant des règles pour $\wedge$, $\rightarrow$, $\neg$, $\bot$, et $\vee$. Est-ce que c'est suffisant pour prouver toutes les tautologies de la logique propositionnelle ?

Logique intuitionniste et classique

Nous avons maintenant des règles pour $\wedge$, $\rightarrow$, $\neg$, $\bot$, et $\vee$. Est-ce que c'est suffisant pour prouver toutes les tautologies de la logique propositionnelle ?

Considérez $\neg(p \wedge q) \rightarrow \neg p \vee \neg q$. On ne peut pas la prouver !

Les règles que nous avons introduites jusqu'à maintenant définissent la logique intuitionniste. Pour avoir la logique classique, il faut . . .

Tertium non datur

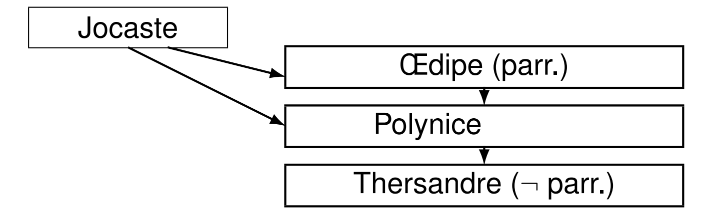
$$\frac{}{\Gamma \vdash A \vee \neg A}\ (TND) \qquad \text{(tertium non datur)}$$

Dans la littérature, on trouve aussi deux autres formulations, mais nous ne discuterons pas cela ...

Exemple du raisonnement classique

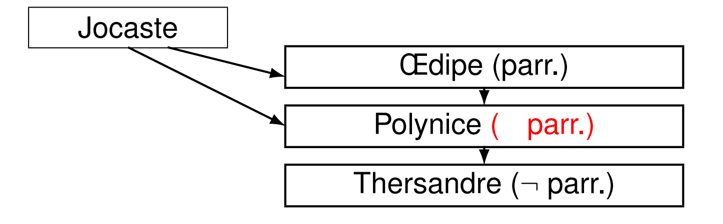
- Jocaste est la mère d'Œdipe.
- Jocaste et Œdipe sont les parents de Polynice.
- Polynice est le père de Thersandre.
- Œdipe est un parricide
- Thersandre n'est pas un parricide.

Exemple du raisonnement classique (2)



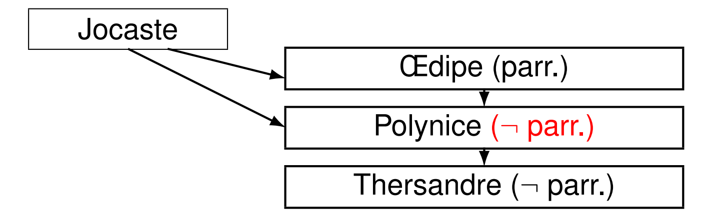
Est-ce que Jocaste a un fils qui est un parricide qui lui-même a un fils qui n'est pas un parricide ?

Exemple du raisonnement classique (2)



Est-ce que Jocaste a un fils qui est un parricide qui lui-même a un fils qui n'est pas un parricide ?
Cas 1 : Si Polynice est un parricide, alors Jocaste a un fils (Polynice) qui est un parricide et qui lui-même a un fils (Thersandre) qui n'est pas un parricide.

Exemple du raisonnement classique (2)



Est-ce que Jocaste a un fils qui est un parricide qui lui-même a un fils qui n'est pas un parricide ?

Cas 2 : Si Polynice n' est pas un parricide, alors Jocaste a un fils (Œdipe) qui est un parricide et qui lui-même a un fils (Polynice) qui n'est pas un parricide.

Preuve de $\neg(p \wedge q) \rightarrow \neg p \vee \neg q$

$$
\dfrac{
\dfrac{}{\Gamma_1 \vdash p \vee \neg p}\;(TND)
\qquad
\dfrac{
\dfrac{
\dfrac{
\Gamma_2 \vdash \neg(p \wedge q)
\quad
\dfrac{\Gamma_2 \vdash p \quad \Gamma_2 \vdash q}{\Gamma_2 \vdash p \wedge q}\;(I\wedge)
}{\Gamma_1, p, q \vdash \bot}\;(E\neg)
}{\Gamma_1, p \vdash \neg q}\;(I\neg)
}{\Gamma_1, p \vdash \neg p \vee \neg q}\;(I\vee_2)
\qquad
\dfrac{\Gamma_1, \neg p \vdash \neg p}{\Gamma_1, \neg p \vdash \neg p \vee \neg q}\;(I\vee_1)
}{
\dfrac{\Gamma_1 \vdash \neg p \vee \neg q}{\vdash \neg(p \wedge q) \rightarrow \neg p \vee \neg q}\;(I \longrightarrow)
}\;(E\vee)
$$

avec :

- $\Gamma_1 = \neg(p \wedge q)$
- $\Gamma_2 = \neg(p \wedge q), p, q$

Quand et comment utiliser (TND)

Il n'est pas facile de savoir quand il faut utiliser (TND) et comment. Une idée : rappelez-vous ce que nous avons dit concernant le $\vee$:

> *Quand vous rencontrez* $\ldots \vdash \phi \vee \psi$ *(pour la première fois), ne faites pas* ($I\vee_1$) *ou* ($I\vee_2$)*, mais essayez plutôt de faire* ($E\vee$)*.*

Mais que faire quand il n'y a aucune sous-formule $\alpha \vee \beta$ dans le contexte ?

Quand et comment utiliser (TND)

Il n'est pas facile de savoir quand il faut utiliser (TND) et comment.
Une idée : rappelez-vous ce que nous avons dit concernant le $\vee$:

> *Quand vous rencontrez $\ldots \vdash \phi \vee \psi$ (pour la première fois), ne faites pas ($I\vee_1$) ou ($I\vee_2$), mais essayez plutôt de faire ($E\vee$).*

Mais que faire quand il n'y a aucune sous-formule $\alpha \vee \beta$ dans le contexte ?
C'est peut-être le moment pour utiliser (TND). Exemple :

$$\dfrac{\dfrac{}{p \longrightarrow q \vdash p \vee \neg p}\,(TND) \quad \dfrac{\ldots}{p \longrightarrow q, p \vdash \neg p \vee q} \quad \dfrac{\ldots}{p \longrightarrow q, \neg p \vdash \neg p \vee q}}{p \longrightarrow q \vdash \neg p \vee q}\,(E\vee)$$

Question

Complétez la dérivation.

Correction et Complétude

On ne le prouve pas ici, mais :

- La déduction naturelle avec les règles ci-dessus est correcte pour LProp : si $\{H_1, \ldots, H_n\} \vdash C$, alors $\{H_1, \ldots, H_n\} \models C$
- La déduction naturelle avec les règles ci-dessus est complète pour LProp : si $\{H_1, \ldots, H_n\} \models C$, alors $\{H_1, \ldots, H_n\} \vdash C$

Déduction Naturelle : Résumé

Principes :

- Motivation : Modéliser le raisonnement humain
- Structure de base : Arbre de dérivation
  - Lecture : De haut en bas (antécédent $\rightsquigarrow$ conséquent)
  - Construction : De bas en haut

Règles :

- …d'introduction : connecteur dans le conséquent
- …d'élimination : connecteur dans l'antécédent

Difficile à automatiser (pas de propriété de sous-formule, il faut inventer des formules)

Déduction Naturelle : Exercices

1. $p \longrightarrow (q \longrightarrow r) \vdash q \longrightarrow (p \longrightarrow r)$
2. $p \longrightarrow (q \longrightarrow r) \vdash (p \longrightarrow q) \longrightarrow (p \longrightarrow r)$
3. $p \longrightarrow q, p \longrightarrow r \vdash p \longrightarrow q \wedge r$
4. $p \longrightarrow q \wedge r \vdash (p \longrightarrow q) \wedge (p \longrightarrow r)$
5. $(p \longrightarrow q) \vdash ((p \wedge q) \leftrightarrow p)$
6. $((p \wedge q) \leftrightarrow p) \vdash (p \longrightarrow q)$
7. $p \longrightarrow r, q \longrightarrow r \vdash p \vee q \longrightarrow r$
8. $p \vee (p \wedge q) \vdash p$
9. $p \wedge (q \vee r) \vdash (p \wedge q) \vee (p \wedge r)$
10. $p \longrightarrow q, \neg q \vdash \neg p$
11. $p \vdash \neg\neg p$
12. $\neg\neg p \vdash p$

Déduction Naturelle : Exercices (2)

13. $\vdash p \vee q \longrightarrow \neg(\neg p \wedge \neg q)$
14. $\vdash \neg(\neg p \wedge \neg q) \longrightarrow p \vee q$
15. $p \wedge q \vdash \neg(\neg p \vee \neg q)$
16. $\neg(\neg p \vee \neg q) \vdash p \wedge q$
17. $\vdash \neg p \vee q \longrightarrow (p \longrightarrow q)$
18. $\vdash q \longrightarrow (p \longrightarrow q) \longrightarrow \neg p \vee q$

Plan

Où en sommes-nous ?

- Nous savons écrire des formules (propositionnelles) : syntaxe
- Nous savons ce que ça veut dire qu'une formule est vraie ou fausse : sémantique
- Nous connaissons une méthode astucieuse pour vérifier qu'une formule est valide : déduction naturelle

Où en sommes-nous ?

- Nous savons écrire des formules (propositionnelles) : syntaxe
- Nous savons ce que ça veut dire qu'une formule est vraie ou fausse : sémantique
- Nous connaissons une méthode astucieuse pour vérifier qu'une formule est valide : déduction naturelle

En bref, nous savons utiliser la logique des propositions.

Où en sommes-nous ?

Maintenant, nous allons nous doter du nécessaire pour étudier la logique des propositions en elle-même, c'est-à-dire des propriétés portant sur l'ensemble des formules

Où en sommes-nous ?

Maintenant, nous allons nous doter du nécessaire pour étudier la logique des propositions en elle-même, c'est-à-dire des propriétés portant sur l'ensemble des formules

- Remplacement d'équivalents
- Correction et complétude de la déduction naturelle ou autre
- ...

Plan

		Lo. prop.	Lo. prédicats	...
Syntaxe		✔☞		
Sémantique		✔☞		
Modélisation		✔		
Méth. preuve	• Déd. nat.	✔		
	• Tableaux			
	• Résolution			

Plan

Induction : histoire



Maurolico (1494-1575)

Première preuve par induction



Peano (1858 - 1932)

Première axiomatisation des nombres naturels

Triade

Nous verrons une “triade” :

- définition inductive d’un ensemble
- fonctions récursives
- preuves par induction

Ici nous ne regardons que les formules propositionnelles, mais il y a d’autres exemples : les nombres naturels, les poupées russes . . .

Exemple : Définition inductive des formules

FORM est le plus petit ensemble qui satisfait les conditions :

1. Variable propositionnelle : Pour tout $p \in PROP$, $p \in FORM$
2. Constante “faux” : $\bot \in FORM$
3. Négation : Si $A \in FORM$, alors $(\neg A) \in FORM$
4. Conjonction (“et”) : Si $A \in FORM$ et $B \in FORM$, alors $(A \wedge B) \in FORM$
5. Disjonction (“ou”) : Si $A \in FORM$ et $B \in FORM$, alors $(A \vee B) \in FORM$
6. Implication (“si ...alors”) : Si $A \in FORM$ et $B \in FORM$, alors $(A \longrightarrow B) \in FORM$

$\Rightarrow$ ici nous avons à la fois des variables (propositionnelles) qui représentent des propositions (p, q,...) et des méta-variables qui représentent des formules (A, B,...). À ne pas confondre !

Définition inductive des formules (2)

Comprendre une définition inductive :

- $s \in PROP$
  - donc $s \in FORM$

Définition inductive des formules (2)

Comprendre une définition inductive :

- $s \in PROP$
  - donc $s \in FORM$
  - donc $(\neg s) \in FORM$

Définition inductive des formules (2)

Comprendre une définition inductive :

- $s \in PROP$
  - donc $s \in FORM$
  - donc $(\neg s) \in FORM$
- $p \in PROP$, et donc $p \in FORM$

Définition inductive des formules (2)

Comprendre une définition inductive :

- $s \in PROP$
  - donc $s \in FORM$
  - donc $(\neg s) \in FORM$
- $p \in PROP$, et donc $p \in FORM$
- $q \in PROP$, et donc $q \in FORM$

Définition inductive des formules (2)

Comprendre une définition inductive :

- $s \in PROP$
  - donc $s \in FORM$
  - donc $(\neg s) \in FORM$
- $p \in PROP$, et donc $p \in FORM$
- $q \in PROP$, et donc $q \in FORM$
- $r \in PROP$, et donc $r \in FORM$

Définition inductive des formules (2)

Comprendre une définition inductive :

- $s \in PROP$
  - donc $s \in FORM$
  - donc $(\neg s) \in FORM$
- $p \in PROP$, et donc $p \in FORM$
- $q \in PROP$, et donc $q \in FORM$
- $r \in PROP$, et donc $r \in FORM$
- donc $(q \vee r) \in FORM$

Définition inductive des formules (2)

Comprendre une définition inductive :

- $s \in PROP$
  - donc $s \in FORM$
  - donc $(\neg s) \in FORM$
- $p \in PROP$, et donc $p \in FORM$
- $q \in PROP$, et donc $q \in FORM$
- $r \in PROP$, et donc $r \in FORM$
- donc $(q \vee r) \in FORM$
- donc $(p \wedge (q \vee r)) \in FORM$



Définition inductive des formules (2)

Comprendre une définition inductive :

- $s \in PROP$
  - donc $s \in FORM$
  - donc $(\neg s) \in FORM$
- $p \in PROP$, et donc $p \in FORM$
- $q \in PROP$, et donc $q \in FORM$
- $r \in PROP$, et donc $r \in FORM$
- donc $(q \vee r) \in FORM$
- donc $(p \wedge (q \vee r)) \in FORM$
- et donc finalement $((p \wedge (q \vee r)) \longrightarrow (\neg s)) \in FORM$



Définition récursive sur les formules

Nous avons déjà vu l'exemple de la définition d'une valuation (interprétation) :

- (Variable) : $I_v(p) = v(p)$
- (Constante) : $I_v(\perp) = 0$
- (Négation) : $I_v(\neg A) = 1 - I_v(A)$
- (Conjonction) : $I_v(A \wedge B) = min(I_v(A), I_v(B))$
- (Disjonction) : $I_v(A \vee B) = max(I_v(A), I_v(B))$
- (Implication) : $I_v(A \longrightarrow B) = max(1 - I_v(A), I_v(B))$

Nous regarderons maintenant un autre exemple ...



Définition récursive : un autre exemple

Exemple : Nous définissons la fonction nbp (nombre de parenthèses) ainsi :

- Variable [eq. V] : $\mathtt{nbp}(\mathtt{p}) = 0$
- Constante [eq. C] : $\mathtt{nbp}(\bot) = 0$
- Négation [eq. N] : $\mathtt{nbp}((\neg A)) = \mathtt{nbp}(A) + 2$
- Conjonction [eq. C] : $\mathtt{nbp}((A \wedge B)) = \mathtt{nbp}(A) + \mathtt{nbp}(B) + 2$
- Disjonction [eq. D] : $\mathtt{nbp}((A \vee B)) = \mathtt{nbp}(A) + \mathtt{nbp}(B) + 2$
- Implication [eq. I] : $\mathtt{nbp}((A \longrightarrow B)) = \mathtt{nbp}(A) + \mathtt{nbp}(B) + 2$

Quelques formules :

- $\mathtt{nbp}(((p \vee q) \wedge r)) = 4$
- $\mathtt{nbp}(((p \wedge q) \vee (\neg(r \vee \bot)))) = 8$



Preuves par induction pour les formules

Schéma d'induction sur les formules :

- base (Variable) : Si $\mathcal{P}(p)$
- base (Constante) : et si $\mathcal{P}(\perp)$
- hérédité (Négation) : et si pour toute formule A, $\mathcal{P}(A)$ implique $\mathcal{P}((\neg A))$
- hérédité (Conjonction) : et si pour tout A, B, $\mathcal{P}(A)$ et $\mathcal{P}(B)$ implique $\mathcal{P}((A \wedge B))$
- hérédité (Disjonction) : et si pour tout A, B, $\mathcal{P}(A)$ et $\mathcal{P}(B)$ implique $\mathcal{P}((A \vee B))$
- hérédité (Implication) : et si pour tout A, B, $\mathcal{P}(A)$ et $\mathcal{P}(B)$ implique $\mathcal{P}((A \longrightarrow B))$
- alors on peut conclure : $\forall A \in FORM.\ \mathcal{P}(A)$



Preuve par induction : exemple

Preuve par induction Exemple : Montrer que le nombre de parenthèses est toujours pair : $\forall f.nbp(f) \mod 2 = 0$

- Identifier le prédicat $\mathcal{P}$: Ici : $\mathcal{P}(A) \equiv (nbp(A) \mod 2 = 0)$
- Cas de base (Variable) : Montrer : $\mathcal{P}(p)$, donc : $nbp(p) \mod 2 = 0 \mod 2 = 0$ (par [eq. V])
- Cas de base (Constante) : Montrer : $\mathcal{P}(\perp)$, donc : $nbp(\perp) \mod 2 = 0 \mod 2 = 0$ (par [eq. C])

Preuve par induction : exemple (suite)

- Hérédité (Négation) : Montrer : si $\mathcal{P}(A)$, alors $\mathcal{P}((\neg A))$
  - Hypothèse d'induction [eq. H] : $nbp(A) \mod 2 = 0$
  - Montrer : $nbp((\neg A)) \mod 2 = 0$. Calculer :
    - $nbp((\neg A)) \mod 2 = (nbp(A) + 2) \mod 2$ (par [eq. N])
    - $= nbp(A) \mod 2$ (arithmétique)
    - $= 0$ (par [eq. H])

Preuve par induction : exemple (suite)

- Hérédité (Conjonction) : Montrer : si $\mathcal{P}(A)$ et $\mathcal{P}(B)$, alors $\mathcal{P}((A \wedge B))$
  - Hypothèses d'induction
    - [eq. H_1] : $nbp(A) \mod 2 = 0$
    - [eq. H_2] : $nbp(B) \mod 2 = 0$
  - Montrer : $nbp((A \wedge B)) \mod 2 = 0$. Calculer :
    - $nbp((A \wedge B)) \mod 2 = (nbp(A) + nbp(B) + 2) \mod 2$ (par [eq. C])
    - $= (nbp(A) \mod 2 + nbp(B) \mod 2) \mod 2$ (arithmétique)
    - $= (0 + nbp(B) \mod 2) \mod 2$ (par [eq. H_1])
    - $= (0 + 0) \mod 2$ (par [eq. H_2])
    - $= 0$ (arithmétique)
- Hérédité (Disjonction et Implication) : Similaire

Induction : résumé

La Triade :

- ensembles inductifs :
  - générés à partir de cas de base,
  - en appliquant des règles de construction
- Fonctions récursives (récursion) :
  - décomposent une structure inductive composée
  - s'arrêtent sur les cas de base

  ...et synthétisent un résultat en remontant
- Preuves par induction : Permettent de conclure qu'une propriété est satisfaite pour tout élément d'un ensemble inductif
  - si elle est satisfaite pour les cas de base
  - si elle est héréditaire pour les éléments composés



Plan

Substitutions (1)

Une substitution remplace toutes les occurrences d'une variable propositionnelle p dans une formule A par une formule C.

Notation : $A[C/p]$

Exemple :

$$
\begin{aligned}
& (q \wedge (p \longrightarrow (\neg p)))[(r \vee s)/p] \\
= \quad & (q[(r \vee s)/p] \wedge (p \longrightarrow (\neg p))[(r \vee s)/p]) \\
= \quad & (q \wedge (p[(r \vee s)/p] \longrightarrow (\neg p)[(r \vee s)/p])) \\
= \quad & (q \wedge ((r \vee s) \longrightarrow (\neg p[(r \vee s)/p]))) \\
= \quad & (q \wedge ((r \vee s) \longrightarrow (\neg (r \vee s))))
\end{aligned}
$$

Substitutions (2)

Contre-exemples (dessinez les arbres syntaxiques !) :

- Pourquoi $(\neg p)[r \lor s/p] \neq (\neg r \lor s)$? ?
- Pourquoi $(p \longrightarrow (\neg p))[(r \lor s)/p] \neq ((r \lor s) \longrightarrow (\neg p))$? ?

Question

- Donner une définition (par récursion sur A) de : $A[C/p]$
- Définir la fonction $nbocc(p, A)$ qui compte le nombre d'occurrences d'une variable propositionnelle p dans A.
- Si $nbocc(p, A) = 0$, alors $A[C/p]$ =??? (preuve !)
- Définir une fonction $taille(A)$ qui calcule la taille d'une formule ($\equiv$ nombre de nœuds de l'arbre syntaxique)

Devoir à la maison / TD

Quel est le rapport entre $taille(A)$, $taille(C)$, $nbocc(p, A)$ et $taille(A[C/p])$? Prouvez par induction !

Correction partielle

Le rapport cherché est :

$$taille(A[C/p]) = taille(A) + nbocc(p, A) \cdot (taille(C) - 1)$$

Correction partielle

Le rapport cherché est :

$$taille(A[C/p]) = taille(A) + nbocc(p, A) \cdot (taille(C) - 1)$$

Preuve : La preuve se fait par induction et se sert des points S1a . . . S6, O1a . . . O6, T1a . . . T6 discutés en cours.

Cas de base 1a

A prouver :

$$taille(p[C/p]) = taille(p) + nbocc(p, p) \cdot (taille(C) - 1)$$

On calcule :

$$\begin{array}{lr} taille(p[C/p]) = & \text{S1a} \\ taille(C) = & \text{“Anti-simplification”} \\ 1 + 1 \cdot (taille(C) - 1) = & \text{T1a} \\ taille(p) + 1 \cdot (taille(C) - 1) = & \text{O1a} \\ taille(p) + nbocc(p, p) \cdot (taille(C) - 1) & \end{array}$$

Correction partielle

Le rapport cherché est :

$$taille(A[C/p]) = taille(A) + nbocc(p, A) \cdot (taille(C) - 1)$$

Preuve : La preuve se fait par induction et se sert des points S1a . . . S6, O1a . . . O6, T1a . . . T6 discutés en cours.

Cas de base 1a

A prouver :

$$taille(p[C/p]) = taille(p) + nbocc(p, p) \cdot (taille(C) - 1)$$

On calcule :

$$\begin{array}{lr} taille(p[C/p]) = & \text{S1a} \\ taille(C) = & \text{“Anti-simplification”} \\ 1 + 1 \cdot (taille(C) - 1) = & \text{T1a} \\ taille(p) + 1 \cdot (taille(C) - 1) = & \text{O1a} \\ taille(p) + nbocc(p, p) \cdot (taille(C) - 1) & \end{array}$$

Comment deviner l'étape de “anti-simplification” de $taille(C)$?



Correction partielle

Le rapport cherché est :

$$taille(A[C/p]) = taille(A) + nbocc(p, A) \cdot (taille(C) - 1)$$

Preuve : La preuve se fait par induction et se sert des points S1a . . . S6, O1a . . . O6, T1a . . . T6 discutés en cours.

Cas de base 1a

A prouver :

$$taille(p[C/p]) = taille(p) + nbocc(p, p) \cdot (taille(C) - 1)$$

On calcule :

$$\begin{array}{lr} taille(p[C/p]) = & \text{S1a} \\ taille(C) = & \text{“Anti-simplification”} \\ 1 + 1 \cdot (taille(C) - 1) = & \text{T1a} \\ taille(p) + 1 \cdot (taille(C) - 1) = & \text{O1a} \\ taille(p) + nbocc(p, p) \cdot (taille(C) - 1) & \end{array}$$

Comment deviner l'étape de “anti-simplification” de $taille(C)$? On ne devine pas, on laisse un trou, on met le résultat attendu $taille(p) + nbocc(p, p) \cdot (taille(C) - 1)$ et on travaille de droite à gauche pour remplir le trou.

Correction partielle (2)

Hérédité 3
Hypothése d'induction (HI) :

$$taille(A[C/p]) = taille(A) + nbocc(p, A) \cdot (taille(C) - 1)$$

A prouver :

$$taille((\neg A)[C/p]) = taille((\neg A)) + nbocc(p, (\neg A)) \cdot (taille(C) - 1)$$

On calcule :

$$\begin{array}{lr}
taille((\neg A)[C/p]) = & \text{S3} \\
taille(\neg(A[C/p])) = & \text{T3} \\
taille(A[C/p]) + 1 = & \text{HI} \\
taille(A) + nbocc(p, A) \cdot (taille(C) - 1) + 1 & \text{O3} \\
taille(A) + nbocc(p, (\neg A)) \cdot (taille(C) - 1) + 1 & \text{T3} \\
(taille((\neg A)) - 1) + nbocc(p, (\neg A)) \cdot (taille(C) - 1) + 1 & \text{Simplification} \\
taille((\neg A)) + nbocc(p, (\neg A)) \cdot (taille(C) - 1) &
\end{array}$$

Ici encore, les étapes O3 et T3 rendent l'expression plus compliquée et au lieu de les deviner, il vaut mieux laisser un trou et simplifier de droite à gauche.



Correction partielle (2)

Hérédité 3
Hypothése d'induction (HI) :

$$taille(A[C/p]) = taille(A) + nbocc(p, A) \cdot (taille(C) - 1)$$

A prouver :

$$taille((\neg A)[C/p]) = taille((\neg A)) + nbocc(p, (\neg A)) \cdot (taille(C) - 1)$$

On calcule :

$taille((\neg A)[C/p]) =$	S3
$taille(\neg(A[C/p])) =$	T3
$taille(A[C/p]) + 1 =$	HI
$taille(A) + nbocc(p, A) \cdot (taille(C) - 1) + 1$	O3
$taille(A) + nbocc(p, (\neg A)) \cdot (taille(C) - 1) + 1$	T3
$(taille((\neg A)) - 1) + nbocc(p, (\neg A)) \cdot (taille(C) - 1) + 1$	Simplification
$taille((\neg A)) + nbocc(p, (\neg A)) \cdot (taille(C) - 1)$	

Ici encore, les étapes O3 et T3 rendent l'expression plus compliquée et au lieu de les deviner, il vaut mieux laisser un trou et simplifier de droite à gauche.
Complétez les cas de base 1b et 2, et le cas d'hérédité 4 (les cas 5 et 6 sont en analogie) !

Plan

Plan

		Lo. prop.	Lo. prédicats	. . .
Syntaxe		✔	☞	
Sémantique		✔		
Modélisation		✔		
Méth. preuve	• Déd. nat.	✔		
	• Tableaux			
	• Résolution			

Motivation (1)

La logique des propositions est limitée en expressivité.

- elle ne permet pas de parler d'individus :
  "Si l'objet $o1$ est bleu, alors $o1$ est aussi rond"
  - Tentative de modélisation : $B \longrightarrow R$
    Problème : Traduire "Si $o1$ est bleu, alors $o1$ est rond et $o2$ carré"
  - Tentative de modélisation : $B1 \longrightarrow R1 \wedge C2$
    Problème : Différence structurelle avec $X \longrightarrow R1 \wedge C2$ ou $B2 \longrightarrow R1 \wedge C2$?
- elle n'est pas concise :
  "Tout objet bleu est rond" (on connaît les objets $o1$, $o2$, $o3$) :
  $(B1 \longrightarrow R1) \wedge (B2 \longrightarrow R2) \wedge (B3 \longrightarrow R3)$
- elle ne permet pas de parler d'une infinité d'individus :
  "Tout objet bleu est rond"
- elle ne permet pas de parler d'actions / opérations :
  "Tout objet repeint deux fois apparaît neuf"



Motivation (2)

La logique des prédicats LPred raffine la logique des propositions.

Individus et prédicats

- Langage naturel : “Si l’objet $o1$ est bleu, alors $o1$ est aussi rond”
- LProp : $B1 \longrightarrow R1$, où
    - $B1, R1$ sont des phrases élémentaires
- LPred : $B(o1) \longrightarrow R(o1)$, où
    - $o1$ est le sujet de la phrase : “l’objet $o1$”
    - B est le prédicat : “est bleu”
    - On garde les connecteurs de LProp ($\longrightarrow$)



Motivation (3)

Quantificateurs

- Langage naturel : “Tout objet bleu est rond”
- LProp : Pas exprimable en général
- LPred : $\forall x.(B(x) \longrightarrow R(x))$

Opérations / Fonctions

- Langage naturel : “Tout objet repeint deux fois apparaît neuf”
- LProp : Pas exprimable en général
- LPred : $\forall x.N(r(r(x)))$, où
  - x est un individu
  - r est une fonction qui transforme des individus (“repeindre”)
  - N est un prédicat



Syntaxe de LPred : Termes et formules

Dans la logique propositionnelle, les expressions syntaxiques étaient les formules (peuvent être vraies ou fausses).

Syntaxe de LPred : Termes et formules

Dans la logique propositionnelle, les expressions syntaxiques étaient les formules (peuvent être vraies ou fausses).

Dans la logique des prédicats, nous avons deux catégories syntaxiques : les termes et les formules. Un terme représente un individu.

Syntaxe de LPred : Termes

Termes : Soit

- VAR un ensemble de variables d'individus
- Pour quelque(s) $n \in \mathbb{N}$, FON_n un ensemble des fonctions n-aires

L'ensemble $TERM$ des termes est défini par induction comme le plus petit ensemble qui satisfait :

1. Variable : si $x \in VAR$, alors $x \in TERM$
2. Application de fonction : si $t_1 \in TERM, \ldots, t_n \in TERM$ et $f \in FON_n$, alors $f(t_1, \ldots, t_n) \in TERM$

On appelle des éléments de FON_0 des constantes.
Souvent, on écrit c au lieu de $c()$.
Exemples : Soient $f \in FON_2$, $x, y \in VAR$, $g \in FON_1$, $\pi \in FON_0$

- $f(x, \pi) \in TERM$
- $f(x, g(f(y, \pi))) \in TERM$



Exercices et explications

Question

Soit $VAR = \{x\}$, $FON_0 = \{0\}$, $FON_1 = \{s\}$, et $FON_i = \emptyset$ pour tout $i \geq 2$.
$TERM = \ldots ?$

Question

Soit $VAR = \emptyset$, $FON_0 = \{luc, ode\}$, $FON_1 = \{pere, mere\}$, et $FON_i = \emptyset$ pour tout $i \geq 2$.
$TERM = \ldots ?$

Question

C'est quoi donc, **le** langage des termes de la logique du premier ordre ?

Syntaxe de LPred : Formules

Formules : Soit $PRED_n$ un ensemble des prédicats n-aires

L'ensemble $FORM$ des formules est défini par induction comme le plus petit ensemble qui satisfait :

1. Application de prédicat : si $t_1 \in TERM, \ldots, t_n \in TERM$ et $P \in PRED_n$, alors $P(t_1, \ldots, t_n) \in FORM$
2. Constante "faux" : $\perp \in FORM$
3. Négation : Si $A \in FORM$,
alors $(\neg A) \in FORM$
4. Connecteurs binaires : Si $A \in FORM$ et $B \in FORM$,
alors $(A \wedge B) \in FORM, (A \vee B) \in FORM, (A \longrightarrow B) \in FORM$
5. Quantificateur universel ("pour tout") : Si $A \in FORM$ et $x \in VAR$,
alors $(\forall x.A) \in FORM$
6. Quantificateur existentiel ("il existe") : Si $A \in FORM$ et $x \in VAR$,
alors $(\exists x.A) \in FORM$

à noter : $FORM$ dépend de $TERM$, mais pas inversement



Exercices

Question

Soit $VAR = \{x, y\}$, $FON_0 = \{0\}$, $FON_1 = \{s\}$, et $FON_i = \emptyset$ pour tout $i \geq 2$, comme ci-dessus, sauf que l'on a ajouté la variable y.
Soit par ailleurs $PRED_0 = \emptyset$, $PRED_1 = \{Pair\}$, $PRED_2 = \{Geq, Eq\}$.
Donnez quelques formules.

Exercices

Question

Soit $VAR = \{x, y\}$, $FON_0 = \{0\}$, $FON_1 = \{s\}$, et $FON_i = \emptyset$ pour tout $i \geq 2$, comme ci-dessus, sauf que l'on a ajouté la variable y.
Soit par ailleurs $PRED_0 = \emptyset$, $PRED_1 = \{Pair\}$, $PRED_2 = \{Geq, Eq\}$.
Donnez quelques formules.

Question

Est-ce que $Eq(Eq(0, 0), Eq(0, 0))$ est une formule ? Pourquoi (pas) ?

Question

Y a-t-il une manière plus "normale" d'écrire $Geq(s(0), 0)$?

Fonctions et Prédicats

Un prédicat ne peut pas prendre des formules comme arguments :
“Eve mange les pommes qu’elle achète” :

- Faux : $Manger(eve, Acheter(eve, pomme))$
- Correct : $(\forall x.(Acheter(eve, x) \longrightarrow Manger(eve, x)))$

Convention : nom de fonctions : minuscules ; de prédicats : majuscules

Convention pour les quantificateurs

Pour ne pas devoir écrire tant de parenthèses, on utilise les mêmes conventions que pour la logique propositionnelle. Or, pour les quantificateurs, on veut aussi une convention efficace qui permet d'écrire moins de parenthèses dans la plupart des cas. Comme précédemment, ce n'est qu'une façon efficace de communiquer une formule selon la définition inductive.

- La formule sans parenthèses $\forall x.A \wedge B$ se lit-elle :
  - $(\forall x.A) \wedge B$, ou
  - $\forall x.(A \wedge B)$?

Convention pour les quantificateurs

Pour ne pas devoir écrire tant de parenthèses, on utilise les mêmes conventions que pour la logique propositionnelle. Or, pour les quantificateurs, on veut aussi une convention efficace qui permet d'écrire moins de parenthèses dans la plupart des cas. Comme précédemment, ce n'est qu'une façon efficace de communiquer une formule selon la définition inductive.

- La formule sans parenthèses $\forall x.A \wedge B$ se lit-elle :
  - $(\forall x.A) \wedge B$, ou
  - $\forall x.(A \wedge B)$?
- Convention : le quantificateur porte sur la plus grande formule possible à partir du point après l'occurrence liante de la variable derrière le quantificateur

Convention pour les quantificateurs

Pour ne pas devoir écrire tant de parenthèses, on utilise les mêmes conventions que pour la logique propositionnelle. Or, pour les quantificateurs, on veut aussi une convention efficace qui permet d'écrire moins de parenthèses dans la plupart des cas. Comme précédemment, ce n'est qu'une façon efficace de communiquer une formule selon la définition inductive.

- La formule sans parenthèses $\forall x.A \wedge B$ se lit-elle :
  - $(\forall x.A) \wedge B$, ou
  - $\forall x.(A \wedge B)$?
- Convention : le quantificateur porte sur la plus grande formule possible à partir du point après l'occurrence liante de la variable derrière le quantificateur
- Dans l'exemple, ça donne $\forall x.(A \wedge B)$
- Exemples supplémentaires :
  - $((\forall x.A) \longrightarrow (\forall y.B)) \rightsquigarrow (\forall x.A) \longrightarrow \forall y.B$
  - $(\forall x.(A \longrightarrow (\forall y.B))) \rightsquigarrow \forall x.A \longrightarrow \forall y.B$

Modélisation

Soit $VAR = \{x, y, \ldots\}$, $FON_0 = \{luc, jean, eve, marie, paul\}$, $FON_1 = \{pere, mere\}$, $PRED_1 = \{Jeune\}$ $PRED_2 = \{=\}$.

Exemple : “Tous les grand-pères sont vieux” se traduit par $\forall x. \neg Jeune(pere(mere(x))) \land \neg Jeune(pere(pere(x)))$

Traduisez en logique des prédicats les phrases suivantes :

Question

- Eve est la mère de Jean.
- Luc et Eve sont un couple de parents
- . . . (chacun qui propose une réponse a le droit de proposer un nouveau problème — mais pas trop compliqué SVP)

Traduisez en français les formules suivantes :

- $\exists x, y.\ Jeune(x) \land x = mere(y)$
- $\forall x.\ \neg luc = pere(x)$
- . . .

Modélisation (2)

Devoir à la maison / TD

Faites des exercices similaires avec le langage $VAR = \{x, y, \ldots\}$, $FON_0 = \{luc, jean, eve, marie, paul\}$, $PRED_1 = \{Jeune, Fem, Masc\}$, $PRED_2 = \{Parent\}$.

Exemple : “Tous les grand-pères sont vieux” se traduit par
$\forall x.(Masc(x) \wedge \exists y, z.Parent(x, y) \wedge Parent(y, z)) \longrightarrow \neg Jeune(x)$.

Limites de l'expressivité

Contournables : par exemple : propriétés temporelles :

- "Si le composant tombe en panne, il finit par émettre un signal"
- Peut être codé par :
  $\forall t.Panne(c,t) \longrightarrow (\exists t'.t' > t \wedge Signal(c,t'))$

Essentielles :

- Utilisation des fonctions comme objets :
  - Quantification sur des fonctions : "Toute fonction a une inverse" :
    Interdit : $\forall f.\exists g.\forall x.f(g(x)) = x$
  - Fonctions qui prennent des fonctions comme argument :
    Interdit : $\forall f.\forall x.f(inv(f,x)) = x$
- De même : Quantification sur des prédicats ou ensembles

$\rightsquigarrow$ inapproprié pour raisonner sur certains programmes fonctionnels



Variables libres et variables liées

- Toute occurrence d'une variable dans une formule est liée ou libre ou liante.
- Example :
  $(Q(x) \vee \exists x. \forall y. P(f(x), z) \wedge Q(y)) \vee \forall x. R(x, z, g(x))$

Variables libres et variables liées

- Toute occurrence d'une variable dans une formule est liée ou libre ou liante.
- Example :
  $(Q(x) \lor \exists x. \forall y. P(f(x), z) \land Q(y)) \lor \forall x. R(x, z, g(x))$
  Liées ?

Variables libres et variables liées

- Toute occurrence d'une variable dans une formule est liée ou libre ou liante.
- Example :
  $(Q(x) \vee \exists x. \forall y. P(f(x), z) \wedge Q(y)) \vee \forall x. R(x, z, g(x))$
  Liées ?

Devoir à la maison / TD

Variables libres et variables liées

- Toute occurrence d'une variable dans une formule est liée ou libre ou liante.
- Example :
  $(Q(x) \vee \exists x. \forall y. P(f(x), z) \wedge Q(y)) \vee \forall x. R(x, z, g(x))$
  Liées ? Libres ?

Devoir à la maison / TD

Variables libres et variables liées

- Toute occurrence d'une variable dans une formule est liée ou libre ou liante.
- Example :
  $(Q(x) \vee \exists x.\forall y.P(f(x), z) \wedge Q(y)) \vee \forall x.R(x, z, g(x))$
  Liées ? Libres ?

Devoir à la maison / TD

Variables libres et variables liées

- Toute occurrence d'une variable dans une formule est liée ou libre ou liante.
- Example :
  $(Q(x) \vee \exists x. \forall y. P(f(x), z) \wedge Q(y)) \vee \forall x. R(x, z, g(x))$
  Liées ? Libres ? Liantes ?

Devoir à la maison / TD

Variables libres et variables liées

- Toute occurrence d'une variable dans une formule est liée ou libre ou liante.
- Example :
  $(Q(x) \lor \exists x. \forall y. P(f(x), z) \land Q(y)) \lor \forall x. R(x, z, g(x))$
  Liées ? Libres ? Liantes ?
- Une formule sans occurrences libres de variables est close.

Devoir à la maison / TD

Variables libres et variables liées

- Toute occurrence d'une variable dans une formule est liée ou libre ou liante.
- Example :
  $(Q(x) \vee \exists x.\, \forall y.\, P(f(x), z) \wedge Q(y)) \vee \forall x.\, R(x, z, g(x))$
  Liées ? Libres ? Liantes ?
- Une formule sans occurrences libres de variables est close.

Nous écrivons : $fv(F)$ pour les variables libres dans F.

Devoir à la maison / TD

Marquez les occurrences dans la formule suivante :

$$(\forall y.P(y,x) \longrightarrow \exists x.\exists z.R(x,z)) \vee R(y,z) \wedge \exists z.Q(y,z)$$

Pour chaque occurrence liée, marquez avec une flèche le quantificateur qui la lie.

Substitutions, début

- Substitution dans un terme :
  $t[s/x]$, où x est une variable et t et s sont des termes :
  1. Variable : $x[s/x] = s$ et $y[s/x] = y$ pour $y \neq x$
  2. Application de fonction : $f(t_1, \ldots, t_n)[s/x] = f(t_1[s/x], \ldots, t_n[s/x])$

Question

Soit $VAR = \{x, y\}$, $FON_0 = \{0\}$, $FON_1 = \{s\}$, $FON_2 = \{plus\}$ et $FON_i = \emptyset$ pour tout $i \geq 3$. Calculez les substitutions suivantes.

- $plus(s(x), 0)[s(s(0))/x]$
- $plus(s(x), x)[s(s(0))/x]$
- $plus(s(x), s(y))[s(s(y))/x]$
- $((plus(x, x)[plus(y, y)/x])[s(y)/y])[0/y]$



Substitutions, suite

- Substitution dans une formule :
  $F[s/x]$, où x est une variable, s est un terme et F une formule :
  1. Application de prédicat : $P(t_1, \ldots, t_n)[s/x] = P(t_1[s/x], \ldots, t_n[s/x])$
     Ici, on se sert de la substitution dans les termes définie avant.
  2. Const. “faux”, connecteurs propositionnels : comme d'habitude
  3. Quantificateur universel :
     1. $(\forall x.A)[s/x] = (\forall x.A)$– rien à faire puisque x n'est pas libre dans $\forall x.A$
     2. $(\forall y.A)[s/x] = (\forall y.(A[s/x]))$ si $y \notin fv(s)$– le cas typique
     3. $(\forall y.A)[s/x] = (\forall y'.(A[y'/y][s/x]))$ si $y \in fv(s)$, où y' est une variable “fraîche” (c.-à-d. $y' \notin fv(s), y' \notin fv(A)$)– cf. diapo suivant
  4. Quantificateur existentiel : En analogie avec $\forall$

Substitutions, fin

Le renommage dans le troisième cas pour les quantificateurs assure qu'une substitution soit saine : la variable quantifiée y diffère des variables de s.
Autrement on aurait $(\forall y.R(y, x))[f(y)/x] = (\forall y.R(y, f(y)))$, donc l'occurrence libre dans $f(y)$ serait capturée par accident.

Substitutions, fin

Le renommage dans le troisième cas pour les quantificateurs assure qu'une substitution soit saine : la variable quantifiée y diffère des variables de s.
Autrement on aurait $(\forall y.R(y,x))[f(y)/x] = (\forall y.R(y,f(y)))$, donc l'occurrence libre dans $f(y)$ serait capturée par accident.
En réalité, on a $(\forall y.R(y,x))[f(y)/x] = (\forall y'.R(y',f(y)))$

Question

Calculer les substitutions de :

- $(\forall x.\exists y.R(x,y) \wedge P(z))[f(v)/z]$
- $(\forall x.\exists y.R(x,y) \wedge P(z))[f(x)/z]$
- $(\forall x.\exists y.R(x,y) \wedge P(z))[f(v)/x]$

Plan

Pas fait en 2021/2022

Plan

Plan

		Lo. prop.	Lo. prédicats	...
Syntaxe		✔	✔	
Sémantique		✔	✔	
Modélisation		✔	✔	
Méth. preuve	• Déd. nat.	✔	☞	
	• Tableaux			
	• Résolution			
Outils	• SAToulouse			

Déduction Naturelle pour LPred

Extension de la déduction naturelle pour LProp :

- Les règles pour LProp restent en vigueur
- Nouvelles règles pour les quantificateurs : $(I\exists), (E\exists), (I\forall), (E\forall)$
- Construction d'un arbre de dérivation . . . comme pour LProp

Règles : $(E\forall)$

$$\frac{\Gamma \vdash \forall x.A}{\Gamma \vdash A[t/x]} \ (E\forall)$$

Lecture informelle :

A est vrai pour tout x. Donc, il est vrai en particulier pour un t (que je peux choisir).

Question

Soit $FON_0 = \{luc, ode\}$, $FON_1 = \{pere, mere\}$, $PRED_1 = \{Jeune\}$.
Remplissez les "…" d'au moins 7 manières distinctes :

$$\frac{\Gamma \vdash \forall x.\neg Jeune(pere(mere(x)))}{\Gamma \vdash \ldots} \ (E\forall)$$

Règles : $(I\forall)$

$$\frac{\Gamma \vdash A}{\Gamma \vdash \forall x.A}\ (I\forall)$$

Condition : $x \notin fv(\Gamma)$

Lecture informelle : si A est vrai pour n'importe quel x, alors aussi $\forall x.A$ est vrai.
Avant d'étudier l'importance de la condition, regardons quelques exemples anodins . . .

Exemple

Soit $\Gamma = \forall x.(P(x) \wedge Q(x))$.

$$
\dfrac{
\dfrac{
\dfrac{
\dfrac{}{\Gamma \vdash \forall x.(P(x) \wedge Q(x))}\,(Ax)
}{\Gamma \vdash P(x) \wedge Q(x)}\,(E\forall)
}{\dfrac{\Gamma \vdash P(x)}{\Gamma \vdash \forall x.P(x)}\,(I\forall)}\,(E\wedge_1)
\qquad
\dfrac{
\dfrac{
\dfrac{}{\Gamma \vdash \forall x.(P(x) \wedge Q(x))}\,(Ax)
}{\Gamma \vdash P(x) \wedge Q(x)}\,(E\forall)
}{\dfrac{\Gamma \vdash Q(x)}{\Gamma \vdash \forall x.Q(x)}\,(I\forall)}\,(E\wedge_2)
}{\Gamma \vdash (\forall x.P(x)) \wedge (\forall x.Q(x))}\,(I\wedge)
$$

Exercices

Question

$(\forall x.P(x)) \wedge (\forall x.Q(x)) \vdash \forall x.(P(x) \wedge Q(x))$

Devoir à la maison / TD

$(\forall x.P(x)) \vee (\forall x.Q(x)) \vdash \forall x.(P(x) \vee Q(x))$

Question

$P(0), \forall x.P(x) \longrightarrow P(s(s(x))) \vdash P(s(s(s(s(0)))))$

$(I\forall)$: l'importance de la condition

Voilà une tentative de dériver $\forall x.(H(x) \vee F(x)) \vdash (\forall x.H(x)) \vee (\forall x.F(x))$ (H= "Homme", F= "Femme") :

$$
\dfrac{
\dfrac{\dfrac{}{\Gamma \vdash \forall x.H(x) \vee F(x)}\,(Ax)}{\Gamma \vdash H(x) \vee F(x)}\,(E\forall)
\qquad
\dfrac{\dfrac{\dfrac{}{\Gamma_P \vdash H(x)}\,(Ax)}{\Gamma_P \vdash \forall x.H(x)}\,(I\forall)}{\Gamma_P \vdash (\forall x.H(x)) \vee (\forall x.F(x))}\,(I\vee_1)
\qquad
\dfrac{\dots}{\Gamma_Q \vdash \dots}\,(I\vee_2)
}{\Gamma \vdash (\forall x.H(x)) \vee (\forall x.F(x))}\,(E\vee)
$$

où $\Gamma = \forall x.H(x) \vee F(x)$ et $\Gamma_P = \Gamma, H(x)$ et $\Gamma_Q = \Gamma, F(x)$.

$(I\forall)$: l'importance de la condition

Voilà une tentative de dériver $\forall x.(H(x) \vee F(x)) \vdash (\forall x.H(x)) \vee (\forall x.F(x))$ (H= “Homme”, F= “Femme”) :

$$\dfrac{\dfrac{\dfrac{}{\Gamma \vdash \forall x.H(x) \vee F(x)}(Ax)}{\Gamma \vdash H(x) \vee F(x)}(E\forall) \quad \dfrac{\dfrac{\dfrac{}{\Gamma_P \vdash H(x)}(Ax)}{\Gamma_P \vdash \forall x.H(x)}\color{red}{(I\forall)}}{\Gamma_P \vdash (\forall x.H(x)) \vee (\forall x.F(x))}(I\vee_1) \quad \dfrac{\ldots}{\Gamma_Q \vdash \ldots}(I\vee_2)}{\Gamma \vdash (\forall x.H(x)) \vee (\forall x.F(x))}(E\vee)$$

où $\Gamma = \forall x.H(x) \vee F(x)$ et $\Gamma_P = \Gamma, H(x)$ et $\Gamma_Q = \Gamma, F(x)$.
C'est une dérivation incorrecte car ne respectant pas la condition d'application de $(I\forall)$. L'objectif de la condition est de ne pas découpler les variables qui se réfèrent au même objet.

Question

Expliquez la dernière phrase sur cet exemple.



Règles : $(I\exists)$

$$\frac{\Gamma \vdash A[t/x]}{\Gamma \vdash \exists x.A}\ (I\exists)$$

Lecture informelle :
A est vrai pour un t. Donc, il existe un x pour lequel A est vrai.

Question

Soit $FON_0 = \{luc, ode\}$, $FON_1 = \{pere, mere\}$, $PRED_1 = \{Jeune\}$.
Remplissez les "..." d'au moins 7 manières distinctes :

$$\frac{\Gamma \vdash \dots}{\Gamma \vdash \exists x.\neg Jeune(x)}\ (I\exists)$$

Règles : ($E\exists$) (1)

$$\frac{\Gamma \vdash \exists x.A \quad \Gamma, A \vdash C}{\Gamma \vdash C}\ (E\exists)$$

Condition : $x \notin fv(\Gamma) \cup fv(C)$

Lecture informelle : Pour montrer C, sachant que $\exists x.A$, il suffit de postuler A (pour un x dont on ne connaît pas l'identité exacte) et de montrer C.

Règles : ($E\exists$) (2)

Exemple d'une preuve :

$$
\dfrac{\dfrac{}{\Gamma_1 \vdash \exists x.(P(x) \land Q(x))}(Ax) \quad \dfrac{\dfrac{\dfrac{}{\Gamma_2 \vdash P(x) \land Q(x)}(Ax)}{\Gamma_2 \vdash P(x)}(E\land_1)}{\Gamma_1, (P(x) \land Q(x)) \vdash \exists x.P(x)}(I\exists)}{\dfrac{(\exists x.(P(x) \land Q(x))) \vdash \exists x.P(x)}{\vdash (\exists x.(P(x) \land Q(x))) \longrightarrow (\exists x.P(x))}(I \longrightarrow)}(E\exists)
$$

avec

- $\Gamma_1 = (\exists x.(P(x) \land Q(x)))$
- $\Gamma_2 = \Gamma_1, (P(x) \land Q(x))$

Exercices

Question

$\exists x.(P(x) \lor Q(x)) \vdash (\exists x.P(x)) \lor (\exists x.Q(x))$

Devoir à la maison / TD

$(\exists x.P(x)) \lor (\exists x.Q(x)) \vdash \exists x.(P(x) \lor Q(x))$

Question

$\exists x.(P(x) \land Q(x)) \vdash (\exists x.P(x)) \land (\exists x.Q(x))$

$(E\exists)$: l'importance de la condition

Exemple d'une preuve incorrecte(!) :

$$\dfrac{\dfrac{\dfrac{\dfrac{}{(\exists x.P(x)) \vdash \exists x.P(x)}\ (Ax) \quad \dfrac{}{(\exists x.P(x)), P(x) \vdash P(x)}\ (Ax)}{(\exists x.P(x)) \vdash P(x)}\ (E\exists)}{(\exists x.P(x)) \vdash \forall x.P(x)}\ (I\forall)}{\vdash (\exists x.P(x)) \longrightarrow (\forall x.P(x))}\ (I \longrightarrow)$$

Question

1. Est-ce que l'application de $(I\forall)$ est correcte ? Pourquoi ?
2. Est-ce que l'application de $(E\exists)$ est correcte ? Pourquoi ?

Exercices

Question

$\neg(\exists x.P(x)) \vdash \forall x.\neg P(x)$

Devoir à la maison / TD

$\forall x.\neg P(x) \vdash \neg(\exists x.P(x))$

Question

$\neg(\forall x.P(x)) \vdash \exists x.\neg P(x)$ (très difficile !)

Devoir à la maison / TD

$\exists x.\neg P(x) \vdash \neg(\forall x.P(x))$

Devoir à la maison / TD

Essayez $(\exists x.P(x)) \wedge (\exists x.Q(x)) \vdash \exists x.(P(x) \wedge Q(x))$ et identifiez où ça casse !

Logique des prédicats : Résumé

- La logique des prédicats est beaucoup plus expressive que la logique propositionnelle :
  - Elle permet de parler d'individus ;
  - Elle permet de parler d'une infinité d'individus ;
  - Elle est plus concise . . .

Logique des prédicats : Résumé

- La logique des prédicats est beaucoup plus expressive que la logique propositionnelle :
  - Elle permet de parler d'individus ;
  - Elle permet de parler d'une infinité d'individus ;
  - Elle est plus concise . . .
- On a maintenant deux catégories syntaxiques : les termes et les formules.
- On a les quantificateurs $\forall, \exists$ et on introduit quatre règles de dérivation pour traiter $\forall, \exists$ dans la déduction naturelle.

Logique des prédicats : Résumé

- La logique des prédicats est beaucoup plus expressive que la logique propositionnelle :
  - Elle permet de parler d'individus ;
  - Elle permet de parler d'une infinité d'individus ;
  - Elle est plus concise . . .
- On a maintenant deux catégories syntaxiques : les termes et les formules.
- On a les quantificateurs $\forall, \exists$ et on introduit quatre règles de dérivation pour traiter $\forall, \exists$ dans la déduction naturelle.
- La logique des prédicats est la logique “par excellence” :
  - Il y a des logiques plus expressives, mais elles sont beaucoup moins connues.
  - Il y a d'autres logiques (modale, temporelle, descriptive . . .) qui peuvent être traduites dans la logique des prédicats.

